

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 3 年 1 1 月 2 8 日

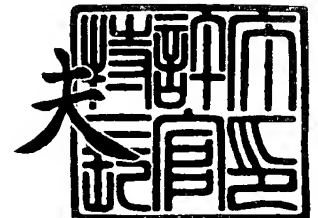
出 願 番 号
Application Number: 特 願 2 0 0 3 - 4 0 0 7 2 4
[ST. 10/C]: [J P 2 0 0 3 - 4 0 0 7 2 4]

出 願 人
Applicant(s): 株式会社東芝

2 0 0 4 年 2 月 3 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願
【整理番号】 A000304099
【提出日】 平成15年11月28日
【あて先】 特許庁長官 殿
【国際特許分類】 H04L 12/00
【発明者】
 【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝研究開発セ
 ンター内
 【氏名】 崎山 伸夫
【発明者】
 【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝研究開発セ
 ンター内
 【氏名】 吉田 英樹
【特許出願人】
 【識別番号】 000003078
 【氏名又は名称】 株式会社 東芝
【代理人】
 【識別番号】 100058479
 【弁理士】
 【氏名又は名称】 鈴江 武彦
 【電話番号】 03-3502-3181
【選任した代理人】
 【識別番号】 100091351
 【弁理士】
 【氏名又は名称】 河野 哲
【選任した代理人】
 【識別番号】 100088683
 【弁理士】
 【氏名又は名称】 中村 誠
【選任した代理人】
 【識別番号】 100108855
 【弁理士】
 【氏名又は名称】 蔵田 昌俊
【選任した代理人】
 【識別番号】 100084618
 【弁理士】
 【氏名又は名称】 村松 貞男
【選任した代理人】
 【識別番号】 100092196
 【弁理士】
 【氏名又は名称】 橋本 良郎
【先の出願に基づく優先権主張】
 【出願番号】 特願2003- 96946
 【出願日】 平成15年 3月31日
【手数料の表示】
 【予納台帳番号】 011567
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1

【物件名】 図面 1
【物件名】 要約書 1
【包括委任状番号】 9705037

【書類名】 特許請求の範囲**【請求項 1】**

サーバからクライアントへ送信されるコンテンツを受信する受信手段と、
受信した前記コンテンツから、不正の機能を有する可能性のあるスクリプトプログラムを抽出する抽出手段と、

前記抽出手段により前記スクリプトプログラムが抽出された場合に、前記コンテンツの送信を許可するか否かについて判断する判断手段と、

前記判断手段により許可すると判断された場合にのみ、前記コンテンツを前記クライアントへ向けて送信する送信手段とを備えたことを特徴とする通信中継装置。

【請求項 2】

前記抽出手段は、受信した前記コンテンツから、前記クライアント又は前記コンテンツに格納されている情報を前記クライアントから送信させる機能を有するスクリプトプログラムを抽出することを特徴とする請求項 1 に記載の通信中継装置。

【請求項 3】

前記情報の正当な送信先として指定されたものを示す送信先情報を記憶する記憶手段を更に備え、

前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記情報の送信先が、前記送信先情報により示される送信先に該当するものでない場合に、前記コンテンツの送信を許可しないと判断することを特徴とする請求項 2 に記載の通信中継装置。

【請求項 4】

前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記情報の送信先が複数存在する場合には、該複数の送信先の全てが前記送信先情報により示される送信先に該当するものであるときにのみ、前記コンテンツの送信を許可すると判断することを特徴とする請求項 3 に記載の通信中継装置。

【請求項 5】

前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記情報の送信先の特定が困難な場合には、該送信先を任意の送信先とみなすことを特徴とする請求項 3 に記載の通信中継装置。

【請求項 6】

前記サーバは、W e b サーバであり、

前記情報は、前記クライアント上で実行中の W e b ブラウザに保持されているクッキー情報を含むものであることを特徴とする請求項 3 に記載の通信中継装置。

【請求項 7】

前記抽出手段は、受信した前記コンテンツから、前記コンテンツに格納されている入力フォームの送信先を示す情報を変更する機能を有するスクリプトプログラムを抽出することを特徴とする請求項 1 に記載の通信中継装置。

【請求項 8】

前記入力フォームの正当な送信先として指定されたものを示す送信先情報を記憶する記憶手段を更に備え、

前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記入力フォームの変更後の送信先が、前記送信先情報により示される送信先に該当するものでない場合に、前記コンテンツの送信を許可しないと判断することを特徴とする請求項 7 に記載の通信中継装置。

【請求項 9】

前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記入力フォームの変更後の送信先が複数存在する場合には、該複数の変更後の送信先の全てが前記送信先情報により示される送信先に該当するものであるときにのみ、前記コンテンツの送信を許可すると判断することを特徴とする請求項 8 に記載の通信中継装置。

【請求項 1 0】

前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記入力フォーム

の変更後の送信先の特定が困難な場合には、該送信先を任意の送信先とみなすことを特徴とする請求項 8 に記載の通信中継装置。

【請求項 1 1】

前記抽出手段は、受信した前記コンテンツから、前記コンテンツに替えて前記サーバと同一又は異なるサーバ上の他のコンテンツを前記クライアントに要求させる機能を有するスクリプトプログラムを抽出することを特徴とする請求項 1 に記載の通信中継装置。

【請求項 1 2】

前記抽出手段は、受信した前記コンテンツから、前記コンテンツに加えて前記サーバと同一又は異なる上の他のコンテンツを前記クライアントから要求させる機能と両コンテンツを一体に表現する機能を有するスクリプトプログラムを抽出することを特徴とする請求項 1 に記載の通信中継装置。

【請求項 1 3】

前記他のコンテンツの正当な要求先として指定されたものを示す要求先情報を記憶する記憶手段を更に備え、

前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記他のコンテンツの要求先が、前記要求先情報により示される要求先に該当するものでない場合に、受信した前記コンテンツの送信を許可しないと判断することを特徴とする請求項 1 1 または 1 2 に記載の通信中継装置。

【請求項 1 4】

前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記他のコンテンツの要求先が複数存在する場合には、該複数の要求先の全てが前記要求先情報により示される要求先に該当するものであるときにのみ、受信した前記コンテンツの送信を許可すると判断することを特徴とする請求項 1 3 に記載の通信中継装置。

【請求項 1 5】

前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記他のコンテンツの要求先の特定が困難な場合には、該要求先を任意の要求先とみなすことを特徴とする請求項 1 3 に記載の通信中継装置。

【請求項 1 6】

前記抽出手段は、受信した前記コンテンツから、前記コンテンツに入力フォームを追加する機能を有するスクリプトプログラムを抽出することを特徴とする請求項 1 に記載の通信中継装置。

【請求項 1 7】

前記入力フォームの正当な送信先として指定されたものを示す送信先情報を記憶する記憶手段を更に備え、

前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記入力フォームの送信先が、前記送信先情報により示される送信先に該当するものでない場合に、前記コンテンツの送信を許可しないと判断することを特徴とする請求項 1 6 に記載の通信中継装置。

【請求項 1 8】

前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記入力フォームの送信先が複数存在する場合には、該複数の送信先の全てが前記送信先情報により示される送信先に該当するものであるときにのみ、前記コンテンツの送信を許可すると判断することを特徴とする請求項 1 7 に記載の通信中継装置。

【請求項 1 9】

前記判断手段は、前記スクリプトプログラムの有する前記機能に係る前記入力フォームの送信先の特定が困難な場合には、該送信先を任意の送信先とみなすことを特徴とする請求項 1 7 に記載の通信中継装置。

【請求項 2 0】

前記送信先情報は、前記許可をする URL のリスト又は正規表現記述を含むものであることを特徴とする請求項 3、8 または 1 7 に記載の通信中継装置。

【請求項 2 1】

前記要求先情報は、前記許可をする URL のリスト又は正規表現記述を含むものであることを特徴とする請求項 1 3 に記載の通信中継装置。

【請求項 2 2】

前記抽出手段は、

前記コンテンツから予め定められた言語により記述されたスクリプトプログラムを検出する手段と、

前記言語により記述されたスクリプトプログラムが検出された場合に、該スクリプトプログラムが前記機能を有するか否かについて判断する手段とを更に備えたことを特徴とする請求項 1 に記載の通信中継装置。

【請求項 2 3】

前記抽出手段は、

検出された前記言語により記述されたスクリプトプログラムが、前記機能を有しないと判断された場合に、該スクリプトプログラムが文書生成するものか否かについて判断する手段と、

前記言語により記述されたスクリプトプログラムが文書生成するものと判断された場合に、該スクリプトプログラムを実行する手段と、

前記実行によって生成された文書から、前記予め定められた言語により記述されたスクリプトプログラムを検出する手段とを更に備えたことを特徴とする請求項 2 2 に記載の通信中継装置。

【請求項 2 4】

前記抽出手段は、

前記コンテンツから予め定められた言語により記述された文書を検出する文書検出手段と、

前記言語により記述された文書が検出された場合に、該文書から予め定められた言語により記述されたスクリプトプログラムを検出するスクリプトプログラム検出手段と、

前記言語により記述されたスクリプトプログラムが検出された場合に、該スクリプトプログラムが前記機能を有するか否かについて判断する手段とを更に備えたことを特徴とする請求項 1 に記載の通信中継装置。

【請求項 2 5】

前記抽出手段は、

検出された前記言語により記述されたスクリプトプログラムが、前記機能を有しないと判断された場合に、該スクリプトプログラムが文書生成するものか否かについて判断する手段と、

前記言語により記述されたスクリプトプログラムが文書生成するものと判断された場合に、該スクリプトプログラムを実行する手段とを更に備え、

前記スクリプトプログラム検出手段は、前記実行によって生成された文書から、前記予め定められた言語により記述されたスクリプトプログラムを検出することを特徴とする請求項 2 4 に記載の通信中継装置。

【請求項 2 6】

前記送信手段は、前記判断手段により許可しないと判断された場合には、前記コンテンツを前記クライアントへ向けて送信しないことを特徴とする請求項 1 に記載の通信中継装置。

【請求項 2 7】

前記送信手段は、前記判断手段により許可しないと判断された場合には、前記コンテンツの代わりに、エラー用コンテンツを前記クライアントへ向けて送信することを特徴とする請求項 2 6 に記載の通信中継装置。

【請求項 2 8】

前記送信手段は、前記判断手段により許可しないと判断された場合には、その旨を通知するメッセージを、予め定められた管理者のアカウント宛てて送信することを特徴とする

る請求項 2 6 に記載の通信中継装置。

【請求項 2 9】

前記送信手段は、前記メッセージに、少なくとも前記コンテンツを付加して送信することを特徴とする請求項 2 8 に記載の通信中継装置。

【請求項 3 0】

前記判断手段を除いて前記通信中継装置を第 1 の計算機上に構成するとともに、前記判断手段を第 2 の計算機上に構成することを特徴とする請求項 1 に記載の通信中継装置。

【請求項 3 1】

前記サーバは、W e b サーバであり、

前記通信中継装置を、前記 W e b サーバに含まれる機能拡張モジュールとして構成することを特徴とする請求項 1 に記載の通信中継装置。

【請求項 3 2】

サーバからクライアントへ送信されるコンテンツを受信するステップと、

受信した前記コンテンツから、不正の機能を有する可能性のあるスクリプトプログラムを抽出するステップと、

前記スクリプトプログラムが抽出された場合に、前記コンテンツの送信を許可するか否かについて判断するステップと、

許可すると判断された場合にのみ、前記コンテンツを前記クライアントへ向けて送信するステップとを有することを特徴とする通信中継方法。

【請求項 3 3】

コンピュータを通信中継装置として機能させるためのプログラムであって、

サーバからクライアントへ送信されるコンテンツを受信する受信機能と、

受信した前記コンテンツから、不正の機能を有する可能性のあるスクリプトプログラムを抽出する抽出機能と、

前記抽出機能により前記スクリプトプログラムが抽出された場合に、前記コンテンツの送信を許可するか否かについて判断する判断機能と、

前記判断機能により許可すると判断された場合にのみ、前記コンテンツを前記クライアントへ向けて送信する送信機能とを実現させるためのプログラム。

【書類名】明細書

【発明の名称】通信中継装置、通信中継方法及びプログラム

【技術分野】

【0001】

本発明は、クライアントとサーバとの間で転送されるコンテンツを中継する通信中継装置、通信中継方法及びプログラムに関する。

【背景技術】

【0002】

インターネットでのWebアクセスに用いられるプロトコルであるHTTPは、要求に応じてコンテンツを返すことで完結する単純なプロトコルであり複数の要求にまたがる状態を持たない。従って、そのままではWebサーバは各Webブラウザを区別することができない。一方、現実の応用では各Webブラウザを区別して認証を行ったり複数のHTTPにまたがって状態を保持したセッションを維持したりする必要があり、このためにクッキー(Cookie)と呼ばれるメカニズムが用いられてきた。

【0003】

クッキーはWebサーバで任意に解釈できる文字列であり、WebブラウザからのHTTPによる要求に対する応答のなかでWebサーバから送信されてWebブラウザ中に設定され、Webブラウザが次回から同一Webサーバ、ないし同一ドメインに属するWebサーバへコンテンツを要求する際に、そのなかに埋め込まれてWebサーバに送信される。クッキーが埋め込まれていない要求への返答に対してWebサーバがそれぞれ異なるクッキー設定の返答を行うことで、Webサーバは各Webブラウザを区別できることになる。

【0004】

一方、Webブラウザで表示される文書の記述技術として、JavaScript(TM)やVBScript(TM)といったスクリプト言語によって記述されたプログラムをHTML中に埋め込んで用いる方法が広く用いられている。Webブラウザで受信されたHTML文書は表示のため内部で解析されて構造を持ったオブジェクトとして扱われるが、このオブジェクトに対してイベントドリブンの操作をスクリプト言語で行うことで動的なコンテンツ表示を行うことを可能としている。これらのスクリプトプログラムはWebサーバにより提供され異なる管理下にあるWebブラウザ上で実行される性質を持つため、通常の状態で操作可能なオブジェクトは表示されるコンテンツやWebブラウザのGUI部品に限定されている。ここで、先に説明したクッキーはWebサーバが設定するものであるため、スクリプトプログラムから自由に操作することができるよう定められている。よって、スクリプトプログラムによるクッキーへの操作によって、クッキー文字列を他のドメインの提携サイトへと転送することによって新たな認証作業をWebブラウザのユーザが行わずにすむシングルサインオンも実装され得る。

【0005】

また、WebブラウザとWebサーバのそれぞれの所有者が特別な関係にありWebサーバを「信頼できる」と判断する場合、Webブラウザの設定により特定のWebサーバからのスクリプトプログラムによってWebブラウザの外のクライアント計算機上のリソースに対する操作を許可することができる。

【0006】

以上のような技術的背景に対するセキュリティ上の脅威として、クロスサイトスクリプティング脆弱性と呼ばれる問題が知られている(例えば、非特許文献1参照)。クロスサイトスクリプティングとは、ユーザが閲覧するWebページに不正なスクリプトプログラムを混入させてユーザのWebブラウザで実行させることで、Webブラウザのクッキーが攻撃者サーバへ漏洩するなどセキュリティ上の被害が発生するものであり、そのような攻撃が有効となるWebシステムはクロスサイトスクリプティング脆弱性を有するとされる。

【0007】

クロスサイトスクリプティング脆弱性の原因は、Webサイトでの動的ページ生成において、ユーザからの入力に由来する内容について十分なチェックが行なわれていないことにあり、チェックを行ない不正スクリプトの無効化を完全に行うことが対策とされている（例えば、非特許文献1参照）。

【0008】

しかし、平均的なWebサイト構築者にとって対策は困難な問題となっている（例えば、非特許文献2参照）。Webサイト構築に用いられるアプリケーションやミドルウェアが脆弱である場合、それらを組み合わせたり設定したりするだけでサイトを運営する場合は脆弱性をチェックするだけの技術をサイト構築者が持たない場合も多く、また仮にWebサイトを構築するプログラムを全て検査しようとした場合、検査項目が膨大になる場合が多いためである。

【0009】

インターネットに接続する計算機の代表的なセキュリティ防護装置としてはファイアウォールが知られているが、クロスサイトスクリプティングはHTTPプロトコル中の形式的には正当なデータによる攻撃であるため、Webサーバを保護するためのファイアウォールによって防ぐことができない。

【0010】

より高度な防御方法としては、侵入検知システムを設置しHTTPのリクエスト内容を細かく検査する方法がある（例えば、非特許文献3, 4参照）が、クロスサイトスクリプティング脆弱性は特定少数の実装がほとんどとなるWebサーバの脆弱性だけではなく、多くのベンダが異なる実装を提供しているミドルウェアさらに個別サイトごとに作られたWebアプリケーションといった広範な領域に関係するため、完全に有効なルールセットを個別サイトの運営に関わらないベンダが提供するのとは不可能であり、また個別サイトにとっても網羅的な検査ルールの作成は脆弱性そのものの除去と同程度のコストがかかると考えられる。

【0011】

ユーザ側での自衛手段として、Webブラウザでのスクリプトプログラム実行全てを禁止する方法があるが、これらはWebサイトの正規のスクリプトプログラムの実行をも禁止するものである上、クロスサイトスクリプティング脆弱性の問題はWebサイト運営上の瑕疵によって生ずるものなので問題の解決とならない。

【0012】

クロスサイトスクリプティングによる被害はクッキー漏洩に留まらず、クッキーの予期しない廃棄やWebサーバを「信頼できるサイト」と設定していた場合のクライアント計算機上のファイルの破壊や漏洩、偽コンテンツの表示などがあげられるが、なかでもクッキーは多くの電子商取引サイトでセッション保持や認証のために利用されており、その漏洩は顧客の個人情報の漏洩や不正取引による金銭的損害に直結する。従って、クッキーの漏洩に注目して対策することは有効である。

【0013】

クッキー漏洩に着目すると、クライアント計算機上にソフトウェアで構成されたファイアウォールによってクッキーの送出を阻止する方法も存在している（例えば、非特許文献5）。しかし、Webサイトの正規のスクリプトプログラムの実行を妨害するものである上、クロスサイトスクリプティング脆弱性の問題はWebサイト運営上の瑕疵によって生ずるものなので、問題の解決とならない。

【0014】

クッキー漏洩へのWebサイトとWebブラウザ双方で連携して行う対策として、WebサーバでクッキーにHTTP-only属性を設定し、WebブラウザでスクリプトプログラムでのHTTP-only属性のついたクッキーの取扱いを禁止するという方式が提案されている（例えば、非特許文献6参照）。しかし、ユーザ側でのWebブラウザの更新が前提とされていること、正当な理由があつてスクリプトによってクッキーを操作する場合には利用できない問題がある。

【0015】

また、クロスサイトスクリプティング脆弱性を利用することによって、Web ページ内のサーバとクライアントとの間以外では秘匿すべき情報を漏洩させることが可能である。さらに、Web ページ内の入力フォームの送信先を不正に変更すること、正当なサイトの Web ページに替えて別の入力フォームをもつ Web ページを表示させること、または正当なサイトの Web ページのなかに別の入力フォームをもつ Web ページを内部フレームを使って表示することによって、ユーザに秘匿すべき情報の入力を促して詐取することが可能である。

【非特許文献 1】「セキュアプログラミング講座 A. WEB プログラマコース」、情報処理振興事業協会 セキュリティセンター、2001 年

【非特許文献 2】「クロスサイトスクリプティング攻撃に対する電子商取引サイトの脆弱さの実態とその対策」、高木浩光 関口智嗣 大蒔和仁、情報処理学会 第 4 回コンピュータセキュリティシンポジウム、2001 年

【非特許文献 3】Abstracting Application-Level Web Security, David Scott and Richard Sharp, the 11th International World-Wide Web conference (WWW2002), 2002

【非特許文献 4】AppShield white paper, Sanctum Inc., 2001

【非特許文献 5】シマンテック 2001 年 9 月 18 日 プレスリリース, <http://www.symantec.co.jp/region/jp/news/year01/010918.html>, 株式会社シマンテック

【非特許文献 6】Mitigating Cross-site Scripting With HTTP-only Cookies, Microsoft, 2002, http://msdn.microsoft.com/workshop/author/dhtml/httponly_cookies.asp

【発明の開示】**【発明が解決しようとする課題】****【0016】**

クロスサイトスクリプティング脆弱性を悪用したクッキーに代表される Web ブラウザに格納される情報の漏洩は顧客の個人情報の漏洩や不正取引による金銭的損害に直結する。責任を負うべき Web サイト管理者にとって、事前に全ての脆弱性を検査して取り除くことは困難である。さらに、既存の脆弱性防御技術によって Web スクリプティングの有用性を損なうことなく完全に対策を行うことは、Web アプリケーションからの脆弱性の完全な除去と同程度に困難であった。また、クロスサイトスクリプティング脆弱性を悪用した Web ページの情報の漏洩やユーザのフォーム入力の詐取も同様に、顧客の個人情報の漏洩や不正取引による金銭的損害に直結する。

【0017】

本発明は、上記事情を考慮してなされたもので、サーバからクライアントに送信されるコンテンツ中に含まれる不正スクリプトを利用した攻撃（例えば、クライアントに格納される情報が漏洩されること、Web ページの内容が漏洩させること、フォーム入力の送信先の変更または虚偽の入力フォームによりユーザのフォーム入力が詐取されることなど）を防止することのできる通信中継装置、通信中継方法及びプログラムを提供することを目的とする。

【課題を解決するための手段】**【0018】**

本発明に係る通信中継装置は、サーバからクライアントへ送信されるコンテンツを受信する受信手段と、受信した前記コンテンツから、不正の機能を有する可能性のあるスクリプトプログラムを抽出する抽出手段と、前記抽出手段により前記スクリプトプログラムが抽出された場合に、前記コンテンツの送信を許可するか否かについて判断する判断手段と、前記判断手段により許可すると判断された場合にのみ、前記コンテンツを前記クライアントへ向けて送信する送信手段とを備えたことを特徴とする。

好ましくは、前記抽出手段は、受信した前記コンテンツから、前記クライアント又は前記コンテンツに格納されている情報を前記クライアントから送信させる機能を有するスク

リプトプログラムを抽出するようにしてもよい。

好ましくは、前記抽出手段は、受信した前記コンテンツから、前記コンテンツに格納されている入力フォームの送信先を示す情報を変更する機能を有するスクリプトプログラムを抽出するようにしてもよい。

好ましくは、前記抽出手段は、受信した前記コンテンツから、前記コンテンツに替えて前記サーバと同一又は異なるサーバ上の他のコンテンツを前記クライアントに要求させる機能を有するスクリプトプログラムを抽出するようにしてもよい。

好ましくは、前記抽出手段は、受信した前記コンテンツから、前記コンテンツに加えて前記サーバと同一又は異なる上の他のコンテンツを前記クライアントから要求させる機能と両コンテンツを一体に表現する機能を有するスクリプトプログラムを抽出するようにしてもよい。

好ましくは、前記抽出手段は、受信した前記コンテンツから、前記コンテンツに入力フォームを追加する機能を有するスクリプトプログラムを抽出するようにしてもよい。

【0019】

本発明では、通信中継装置は、例えば、クライアント（ソフト的には、例えば、Webブラウザ）からの要求を受け付け、サーバ（例えば、Webサーバ）に転送する。サーバから要求に対応するコンテンツが返信されると、例えば、コンテンツのデータタイプを判定するなどして、スクリプトを含み得るデータタイプのものについてはスクリプトを抽出し、検査する。

【0020】

そして、例えば、クライアント情報（例えば、クッキーないしクッキーに由来するデータ等）の送信を試みるスクリプトが含まれると判定されるなどした場合、クライアント情報の送信先をアクセス制御リストと照合するなどして、送信を許可されない送信先（例えば、リストに含まれない送信先）である場合には、コンテンツのクライアントへの送信を禁止する。

【0021】

本発明によれば、クライアントに格納される情報の送信を試みる不正スクリプトがサーバからクライアントへ送信されることを防止でき、これによって、該不正スクリプトによりクライアントに格納される情報が漏洩されること防止することができる。また、この結果、例えばWebサーバ運営者の責任となるセキュリティ被害を防止することができる。さらに、例えば、送信を防止されたスクリプトを含むHTTPセッションについてWebサーバ管理者へ詳細を通知することなどが可能になるため、クロスサイトスクリプティング脆弱性をもつWebアプリケーションやミドルウェアについて修正やアップグレードなどの対策が容易になる。

【0022】

また、例えば、コンテンツ情報（例えば、Webページ中の文字列）の送信を試みるスクリプトやコンテンツ中の入力フォームの送信先（例えば、HTMLフォーマットにおけるformタグのaction属性）の変更を試みるスクリプト、別コンテンツを要求して現コンテンツのかわりに表示するスクリプト、別コンテンツを要求して現コンテンツと一体に表現する（例えば、HTMLフォーマットにおいて別コンテンツのURLをsrc属性としてもつiframeタグを表示する）スクリプトが含まれると判定されるなどした場合、コンテンツ情報の送信先、formの変更後の送信先、別コンテンツの要求先をおのおのアクセス制御リストと照合するなどして、許可されない送信先（例えば、リストに含まれない送信先）である場合には、コンテンツのクライアントへの送信を禁止する。

【0023】

本発明によれば、ユーザとサーバの間でのみ共有されることが期待される秘匿情報の送信・詐取を試みる不正スクリプトがサーバからクライアントへ送信されることを防止でき、これによって、該不正スクリプトにより情報が漏洩されることを防止することができる。また、この結果、例えばWebサーバ運営者の責任となるセキュリティ被害を防止することができる。さらに、例えば、送信を防止されたスクリプトを含むHTTPセッション

についてWebサーバ管理者へ詳細を通知することなどが可能になるため、クロスサイトスクリプティング脆弱性をもつWebアプリケーションやミドルウェアについて修正やアップグレードなどの対策が容易になる。

【0024】

なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムとしても成立し、該プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【発明の効果】

【0025】

本発明によれば、サーバからクライアントに送信されるコンテンツ中に含まれる不正スクリプトを利用した攻撃を防止することができる。

【発明を実施するための最良の形態】

【0026】

以下、図面を参照しながら本発明の実施形態について説明する。

【0027】

以下では、通信中継装置としてネットワーク側通信インタフェースとWebサーバ側通信インタフェースがそれぞれ通信端点となり通信内容を送信するプロキシサーバの形態をとる場合を例にとって説明する。

【0028】

（第1の実施形態）

図1に、本発明の第1の実施形態に係る通信システムの構成例を示す。図1において、1はWebサーバ、2はクライアント計算機、21はクライアント計算機2上で動作するWebブラウザ、3はプロキシサーバ（通信中継装置）、8はネットワーク（本具体例では、インターネットとする）を示す。

【0029】

図1では、1つのWebサーバのみ示しているが、複数のWebサーバが存在し得る。同様に、クライアント計算機2も複数存在し得る。

【0030】

プロキシサーバ3とWebサーバ1との対応関係については、1つのプロキシサーバ2が唯一のWebサーバ1を対象とする構成と、1つのプロキシサーバ3が複数のWebサーバ1を対象にし得る構成とが可能である。

【0031】

図2に、本実施形態のプロキシサーバの構成例を示す。

【0032】

図2に示されるように、本プロキシサーバ3は、（要求元のクライアント計算機2上で動作する）Webブラウザとの通信を行うネットワーク側通信インタフェース31、Webサーバ1との通信を行うWebサーバ側通信インタフェース32、コンテンツ分類部33、文書解釈部34、スクリプト検査部35を備えている。

【0033】

また、スクリプト検査部35は送信許可判定部351を有し、送信許可判定部351は送信許可リスト3511を有する。図3に、送信許可リスト3511の一例を示す。

【0034】

なお、図1では、Webサーバ1とプロキシサーバ3とは、直接接続されるように記述されているが、イントラネットを介して接続してもよいし、インターネットを介して接続するようにしてもよい（後者の場合には、暗号通信等によりセキュリティを確保するのが好ましい）。また、図1では、Webサーバ1とネットワーク8とは、直接接続される

ように記述されているが、例えば、イントラネット経由で接続可能な他の中継装置を介して接続されてもよい。

【0035】

本プロキシサーバは、例えば、計算機によって実現することが可能である。

【0036】

以下、本実施形態の動作の概要について説明する。

【0037】

Webブラウザ（図1のクライアント計算機2参照）は、ネットワーク側通信インタフェース31にTCP/IPにより接続し、HTTPによるリクエストを送信する。本プロキシサーバ3のネットワーク側通信インタフェース31によって受信されたリクエストは、Webサーバ側通信インタフェース32を経由してそのままWebサーバ1へ送られる。Webサーバ1では、リクエストに対応したレスポンスを本プロキシサーバ3のWebサーバ側通信インタフェース32へ送信する。本プロキシサーバ3のWebサーバ側通信インタフェース32では、コンテンツをコンテンツ分類部33へ送る。コンテンツ分類部33では、データ型に応じてスクリプトが含まれ得る型の文書とスクリプトが含まれる可能性がないデータに分類し、スクリプトが含まれる可能性がないデータについてはネットワーク側通信インタフェース31経由でWebブラウザに返信する。スクリプトが含まれ得る型の文書については、各データ型に対応する文書解釈部34へ送る。ただし、文書がスクリプトそのものである場合にはスクリプト検査部35へ送る。

【0038】

本プロキシサーバ3の文書解釈部34では、文書を構文解析する。構文解析の結果、スクリプトを含まない場合は、ネットワーク側通信インタフェース31経由でWebブラウザに返信する。スクリプトを含んでいる場合は、スクリプト検査部35へ送る。スクリプト検査部35では、スクリプトを検査し、Webブラウザに格納される情報に依存するいずれかのデータについて送信を試みるプログラムがあるかどうかを検査し、送信が行われ得る場合には、送信許可判定部351によって送信が許可されるかどうかを判別する。ここでは、送信許可判定部351は、送信先一覧をURLとして保持した送信許可リスト3511を送信許可規則とし照合するものとする。許可されない送信を含む場合は、エラーをネットワーク側通信インタフェース31経由でWebブラウザに送信する。さらに、スクリプトによって動的に文書が生成されるかどうか検査し、動的に文書が生成される場合には、文書解釈部34に結果を送って検査をやり直す。許可されない送信を含まない場合にのみ、スクリプト検査部35はネットワーク側通信インタフェース31経由でWebサーバ1からのレスポンスをWebブラウザへ返信する。

【0039】

以下では、本実施形態のより詳細な動作例について説明するのに先立って、クロスサイトスクリプティング脆弱性によるクッキー漏洩について説明する。

【0040】

なお、ここでは、Webブラウザに格納される情報の一例としてクッキーを考えるものとする。

【0041】

まず、図4を参照しながら、クッキーの典型的利用形態について説明する。図4は、本プロキシサーバにより送信許可される場合である。図4では、本プロキシサーバは省略している。なお、図4では、Webサイトの一例としてオンラインショップを示している（後掲の図5及び図6の同様である）。

【0042】

(1) まず、クライアント計算機から所望のWebサーバへのアクセス・認証がなされる。

(2) 次に、Webサーバからクライアント計算機へ認証用クッキー設定要求がなされる。

(3) 次に、クライアント計算機においてクッキーの設定がなされる。

(4) そして、クライアント計算機からWebサーバへのクッキーつきアクセスがなされる。

【0043】

これによって、WebサーバはWebブラウザを特定する必要のあるサービスを提供できるようになる。

【0044】

次に、図5を参照しながら、提携サイトへのクッキー送信例について説明する。図5は、本プロキシサーバにより送信許可される場合である。図5では、本プロキシサーバは省略している。

【0045】

(1) まず、クライアント計算機とWebサーバAとの間で、図4の(1)～(4)がなされる。

(2) 次に、WebサーバAからクライアント計算機へ「提携サイトBへのクッキー送信スクリプト」の送信がなされる。

(3) 次に、クライアント計算機において「提携サイトBへのクッキー送信スクリプト」が実行され、実行されたスクリプトによって、クライアント計算機からWebサーバBへのクッキー情報の送信・シングルサインオンがなされる。

【0046】

このように、スクリプトプログラムによるクッキーへの操作によって、クッキー情報を他のWebサーバへ送信させ、例えば、新たな認証作業をWebブラウザのユーザが行わずに済むシングルサインオンなどができるようになる。

【0047】

次に、図6を参照しながら、従来の通信システムにおけるクロスサイトスクリプティング脆弱性によるクッキー漏洩について説明する。

【0048】

クロスサイトスクリプティングでは、図5で説明したような仕組みを悪用して、例えば、ユーザが閲覧するWebページに不正なスクリプトプログラムを混入させてユーザのWebブラウザで実行させることで、Webブラウザのクッキー情報を攻撃者サーバへ漏洩させるなどの不正が行われ得る。そして、クッキー情報の漏洩に留まらず、クライアント計算機上のファイルの破壊や漏洩、偽コンテンツの表示なども発生し得る。この不正は、例えば、以下のようにして実現される。

【0049】

ここで、図6のWebサーバ(1a)は、脆弱性を持つものとする(なお、このWebサーバ自体は正当なものである)。また、クライアント計算機は、この脆弱性を持つWebサーバとの間で、例えば、図4のような手順を既に行っており、クッキーを設定しているものとする。

【0050】

(1) まず、攻撃者がクライアント計算機へ不正コンテンツを送付する。これは、例えば、広告メールや、掲示板での誘導など、種々の方法で行われる。

(2) クライアント計算機のWebブラウザが、この不正コンテンツをレンダリングする。

(3) そして、クライアント計算機からWebサーバへ、例えば漏洩先サイトへのクッキー送信スクリプトのもととなるデータ等の不正データを含むGETリクエストを送出してしまう。

(4) このGETリクエストを受けたWebサーバは、誤った出力処理をしてしまう。

(5) この結果、不正スクリプト(漏洩先サイトへのクッキー送信スクリプト)つきHTMLを送付してしまう。

(6) この不正スクリプト(漏洩先サイトへのクッキー送信スクリプト)つきHTMLを受けたクライアント計算機のWebブラウザでは、この不正スクリプトすなわち漏洩先

サイトへのクッキー送信スクリプトを実行してしまう。

(7) この結果、クライアント計算機から漏洩先サイトへのクッキー情報の不正送信がなされてしまう。

(8) このようにして、漏洩先サイト (1 c) は、攻撃したクライアント計算機のクッキー情報を不正に取得することができる。

(9) これによって、漏洩先サイトは、例えば、攻撃したクライアント計算機になりまして、先の Web サーバへアクセスすることができる。

【0051】

これに対して、本実施形態では、図 6 の Web サーバとインターネットとの間に存在するプロキシサーバにおいて、図 6 の (5) の不正スクリプトつき HTML を遮断するようにし、これによって、クッキー情報等の漏洩を防止することができるようにしている。

【0052】

以下、本実施形態のより詳細な動作例について説明する。

【0053】

図 7 及び図 8 に、本実施形態のプロキシサーバ 3 の処理手順の一例を示す。

【0054】

なお、ここでは一例として、スクリプトとして JavaScript 及び VBScript を対象とし、スクリプトを含む可能性のある文書として HTML、XML 及び CSS を対象とするものとする。また、前述のように、Web ブラウザに格納される情報の一例としてクッキーを考えるものとする。

【0055】

Web ブラウザ (図 1 のクライアント計算機 2 参照) からのリクエストが本プロキシサーバ 3 を経由して Web サーバ 1 に送られ、Web サーバ 1 からのレスポンスが本プロキシサーバ 3 で受信される (ステップ S 1)。

【0056】

本プロキシサーバ 3 は、HTTP リクエストを受信すると、当該リクエストが設定された Web サーバへのリクエストであることを確認した上で (ステップ S 2)、Web サーバ 1 へリクエストを送信し (ステップ S 3)、対応する Web サーバ 1 からの HTTP レスポンスを受信する (ステップ S 5)。

【0057】

なお、この一連の過程でエラーが発生した場合は (ステップ S 2 で No の場合、ステップ S 4 で No の場合、ステップ S 6 で No の場合)、エラーコードとエラーメッセージの生成を行って (ステップ S 7)、Web ブラウザへエラーを示すレスポンスを返す (ステップ S 8)。

【0058】

さて、受信 (ステップ S 5) した HTTP レスポンスが HTTP の Message-Body を含んでいない場合は (ステップ S 8)、HTTP レスポンスをそのまま Web ブラウザに送信する形で返信する (ステップ S 9)。

【0059】

次に、HTTP レスポンスの内容はコンテンツ分類部 3 3 に送られる。

【0060】

コンテンツ分類部 3 3 では、HTTP レスポンスの Content-Type ヘッダによって、コンテンツが JavaScript 又は VBScript の場合は (ステップ S 10)、スクリプト検査部 3 5 に、HTML、XML、CSS の場合には (ステップ S 11)、文書解釈部 3 4 へ送る。その他の場合は (ステップ S 10 で No かつステップ S 11 で No の場合)、Web サーバ 1 からの HTTP レスポンスをそのまま Web ブラウザに送信する形で返信する (ステップ S 22)。

【0061】

文書解釈部 3 4 では、文書の型に応じた構文解析を行い (ステップ S 12)、文書が JavaScript 又は VBScript のスクリプトを含む場合は (ステップ S 13)

、スクリプト検査部 3 5 へ送る。スクリプトを含まない場合は（ステップ S 1 3）、Webサーバからの HTTP レスポンスをそのまま Web ブラウザに送信する形で返信する（ステップ S 2 2）。

【0 0 6 2】

スクリプト検査部 3 5 では、スクリプトの構文解析および意味解析を行い、スクリプトで扱うオブジェクトの依存ツリーを作成する（ステップ S 1 4）。

【0 0 6 3】

依存ツリー中で Document オブジェクトの Cookie プロパティが参照され（ステップ S 1 5）、かつ、当該クッキーに依存するデータが別のドキュメントの URL や Form のデータとされている場合（ステップ S 1 6）、それらの URL について送信許可判定部 3 5 1 において送信許可リスト 3 5 1 1 の内容と合致するかどうか検査する。なお、オブジェクトの依存ツリーに対して定数の畳み込みを行っても問題の URL を列挙する形で確定できない場合には、任意の URL への送信であると仮定して検査する（この場合、任意の送信先に対する送信が許可されていないならば、許可されない送信であると判断する）。

【0 0 6 4】

検査においてひとつでも許可リストに合致しない URL がクッキー送信に用いられ得ると判断された場合には（ステップ S 1 7）、当該 Web コンテンツについては送信が許可されないと判断して、当該 Web コンテンツの Web ブラウザ（クライアント計算機 2）への送出を禁止し、検出された当該 Web コンテンツに係る Web ブラウザからの要求及び当該コンテンツを保存して、Web サーバ管理者への通知を目的としたログをとるとともに、該ログ（又は、当該コンテンツのみ若しくは当該要求のみ）を含む通知メッセージを作成し、事前に設定された管理者（アカウント）にメールで送信し（ステップ S 1 6）、また HTTP レスポンスについては、エラーコードとエラーメッセージを生成して（ステップ S 1 9）、Web ブラウザへ返信する（ステップ S 2 2）。

【0 0 6 5】

スクリプト検査部 3 5 では、クッキーの検査とは別に Document オブジェクトの write メソッドが呼び出されているかどうか検査する。Document オブジェクトの write メソッドによって、Web ブラウザによって解釈されるドキュメントが生成されるため、そのなかにスクリプトが含まれていれば実行される可能性があるためである。すなわち、ステップ S 1 5 若しくはステップ S 1 6 又はステップ S 1 7 で No となったものについて、Document オブジェクトの write メソッドが呼び出される場合には（ステップ S 2 0）、スクリプトを部分的に実行する形で新しい文書を作成し（ステップ S 2 1）、文書解釈部 3 4 へ処理を渡してスクリプトが含まれるかどうか検査するところに戻る。

【0 0 6 6】

以上のような検査をへてスクリプトがクッキーの不正送信を行わないと判断できる場合に、Web サーバから受信した HTTP レスポンスを、そのまま Web ブラウザに送信する形で、返信する。

【0 0 6 7】

このように本実施形態によれば、クッキー情報等の漏洩を防止することができる。

【0 0 6 8】

なお、上記では、当該 Web コンテンツについて送信が許可されないと判断された場合に、当該 Web コンテンツの Web ブラウザ（クライアント計算機 2）への送出を禁止するとともに、通知メッセージの送信や、エラーメッセージの送信を行ったが、通知メッセージの送信とエラーメッセージの送信の一方又は両方を行わない構成も可能である（ログを保存しない構成も可能である）。

【0 0 6 9】

なお、上記では、送信許可判定部 3 5 1 は、送信先一覧を URL として保持した送信許可リスト 3 5 1 1 を送信許可規則とし照合する場合を例にとって説明しているが、その代

わりに、許可される送信先URLを正規表現の記述として保有し、個々の送信先URLと照合して全ての送信先URLが正規表現と一致する場合にのみ送信許可の結果を返すようにしてもよいし、両者を併用してもよい。

【0070】

(第2の実施形態)

本発明の第2の実施形態に係る通信システムの構成例は、図1と同様である。

【0071】

図1では、1つのWebサーバのみ示しているが、複数のWebサーバが存在し得る。同様に、クライアント計算機2も複数存在し得る。

【0072】

プロキシサーバ3とWebサーバ1との対応関係については、1つのプロキシサーバ2が唯一のWebサーバ1を対象とする構成と、1つのプロキシサーバ3が複数のWebサーバ1を対象にし得る構成とが可能である。

【0073】

図9に、本実施形態のプロキシサーバの構成例を示す。

【0074】

図9に示されるように、本プロキシサーバ3は、(要求元のクライアント計算機2上で動作する)Webブラウザとの通信を行うネットワーク側通信インタフェース31、Webサーバ1との通信を行うWebサーバ側通信インタフェース32、コンテンツ分類部33、文書解釈部34、スクリプト検査部35を備えている。

【0075】

また、スクリプト検査部35は、クッキー(Cookie)送信許可判定部351、情報送信許可判定部352、フォーム(form)送信先許可判定部353、外部コンテンツ要求先許可判定部354を有する。

【0076】

なお、クッキー(Cookie)送信許可判定部351は、基本的には、第1の実施形態の送信許可判定部351と同様のものである。すなわち、本実施形態では、スクリプト検査部35に、情報送信許可判定部352とフォーム送信先許可判定部353と外部コンテンツ要求先許可判定部354とを付加したものになっている。

【0077】

クッキー送信許可判定部351は、クッキー送信許可リスト3511を有し、情報送信許可判定部352は、情報送信許可リスト3521を有し、フォーム送信先許可判定部353は、フォーム送信先許可リスト3531を有し、外部コンテンツ要求先許可判定部354は、外部コンテンツ要求先許可リスト3541を有する。クッキー送信許可リスト3511の一例、情報送信許可リスト3521の一例、フォーム送信先許可リスト3531の一例および外部コンテンツ要求先許可リスト3541の一例は、図3と同様である。なお、各許可リスト3511, 3521, 3531, 3541の内容は、互いに独立して設定可能であるが、全て同じ内容にしても構わない。

【0078】

なお、図1では、Webサーバ1とプロキシサーバ3とは、直接接続されるように記述されているが、イントラネットを介して接続してもよいし、インターネットを介して接続するようにしてもよい(後者の場合には、暗号通信等によりセキュリティを確保するのが好ましい)。また、図1では、Webサーバ1とネットワーク8とは、直接接続されるように記述されているが、例えば、イントラネット経由で接続可能な他の中継装置を介して接続されてもよい。

【0079】

本プロキシサーバは、例えば、計算機によって実現することが可能である。

【0080】

以下、本実施形態の動作の概要について説明する。

【0081】

Webブラウザ(図1のクライアント計算機2参照)は、ネットワーク側通信インタフェース31にTCP/IPにより接続し、HTTPによるリクエストを送信する。本プロキシサーバ3のネットワーク側通信インタフェース31によって受信されたリクエストは、Webサーバ側通信インタフェース32を経由してそのままWebサーバ1へ送られる。Webサーバ1では、リクエストに対応したレスポンスを本プロキシサーバ3のWebサーバ側通信インタフェース32へ送信する。本プロキシサーバ3のWebサーバ側通信インタフェース32では、コンテンツをコンテンツ分類部33へ送る。コンテンツ分類部33では、データ型に応じてスクリプトが含まれ得る型の文書とスクリプトが含まれる可能性がないデータに分類し、スクリプトが含まれる可能性がないデータについてはネットワーク側通信インタフェース31経由でWebブラウザに返信する。スクリプトが含まれ得る型の文書については、各データ型に対応する文書解釈部34へ送る。ただし、文書がスクリプトそのものである場合にはスクリプト検査部35へ送る。

【0082】

本プロキシサーバ3の文書解釈部34では、文書を構文解析する。構文解析の結果、スクリプトを含まない場合は、ネットワーク側通信インタフェース31経由でWebブラウザに返信する。スクリプトを含んでいる場合は、スクリプト検査部35へ送る。スクリプト検査部35では、スクリプトを検査し、Webブラウザに格納される情報に依存するいずれかのデータについて送信を試みるプログラムがあるかどうかを検査し、送信が行われ得る場合には、クッキー送信許可判定部351によって送信が許可されるかどうかを判別する。ここでは、クッキー送信許可判定部351は、送信先一覧をURLとして保持した送信許可リスト3511を送信許可規則とし照合するものとする。許可されない送信を含む場合は、エラーをネットワーク側通信インタフェース31経由でWebブラウザに送信する。

【0083】

なお、ここまでは、基本的には第1の実施形態と同様である。

【0084】

スクリプト検査部353では、さらに、コンテンツ中の情報の送信を試みるプログラムであるかどうかを検査し、送信が行われうる場合には、情報送信許可判定部352によって送信が許可されるかどうかを判別する。ここでは、情報送信許可判定部352は、送信先一覧をURLとして保持した送信許可リスト3521を送信許可規則とし照合するものとする。許可されない送信を含む場合は、エラーをネットワーク側通信インタフェース31経由でWebブラウザに送信する。さらに、スクリプト検査部35は、formの送信先の変更を試みるプログラムであるかどうかを検査し、変更が行われうる場合には、フォーム送信先許可判定部353によって送信先変更が許可されるかどうかを判別する。ここでは、フォーム送信先許可判定部353は、送信先一覧をURLとして保持した送信先許可リスト3531を送信先許可規則とし照合するものとする。許可されない送信先変更を含む場合は、エラーをネットワーク側通信インタフェース31経由でWebブラウザに送信する。さらに、スクリプト検査部35は、オブジェクトのlocation情報の変更やiframeタグのsrc属性の変更などにより外部コンテンツの表示を試みるプログラムであるかどうかを検査し、変更が行われうる場合には外部コンテンツ要求先許可判定部354によって送信先変更が許可されるかどうかを判別する。ここでは、外部コンテンツ要求先許可判定部354は、要求先一覧をURLとして保持した要求先許可リスト3541を送信先許可規則とし照合するものとする。許可されない送信先変更を含む場合は、エラーをネットワーク側通信インタフェース31経由でWebブラウザに送信する。さらに、スクリプトによって動的に文書が生成されるかどうかを検査し、動的に文書が生成される場合には、formの挿入やiframeタグの挿入が行われるかどうかを検査し、挿入が行われる場合にはformについてはform送信先判定部353により判定を行い、iframeについては、外部コンテンツ要求先許可判定部354により判定を行う。その後、文書検査部34に文書生成の結果を送って検査をやり直す。許可されない送信・送信・外部コンテンツ要求を含まない場合にのみ、スクリプト検査部35はネットワーク

側通信インタフェース 31 経由で Web サーバ 1 からのレスポンスを Web ブラウザへ返信する。

【0085】

以下では、本実施形態のより詳細な動作例について説明するのに先立って、クロスサイトスクリプティング脆弱性によるコンテンツ情報漏洩、form 送信先変更による form 入力詐取、外部偽 form 表示による form 入力情報詐取について説明する。

【0086】

なお、クッキーの典型的利用形態（図 4 参照）、提携サイトへのクッキー送信例（図 5 参照）、クロスサイトスクリプティング脆弱性によるクッキー漏洩（図 6 参照）については、第 1 の実施形態で説明した通りである。

【0087】

まず、図 10 を参照しながら、従来の通信システムにおけるクロスサイトスクリプティング脆弱性によるコンテンツ情報漏洩について説明する。なお、図 10 では、Web サイトの一例としてオンラインショップを示している（後掲の図 11、図 12、図 13 及び図 14 も同様である）。

【0088】

クロスサイトスクリプティングでは、ユーザが閲覧する Web ページに不正なスクリプトプログラムを混入させてユーザの Web ブラウザで実行させることで、セッション中のコンテンツに表記される情報を攻撃者サーバへ漏洩させるなどの不正が行われ得る。

【0089】

ここで、図 10 の Web サーバ（1a）は、脆弱性を持つものとする（なお、この Web サーバ自体は正当なものである）。

【0090】

（1）まず、攻撃者がクライアント計算機へ不正コンテンツを送付する。これは、例えば、広告メールや、掲示板での誘導など、種々の方法で行われる。

（2）クライアント計算機の Web ブラウザが、この不正コンテンツをレンダリングする。

（3）そして、クライアント計算機から Web サーバへ、例えば漏洩先サイトへのコンテンツ情報送信スクリプトのもととなるデータ等の不正データを含む GET リクエストを送出してしまう。

（4）この GET リクエストを受けた Web サーバは、誤った出力処理をしてしまう。

（5）この結果、不正スクリプト（漏洩先サイトへのコンテンツ情報送信スクリプト）つき HTML を送付してしまう。

（6）この不正スクリプト（漏洩先サイトへのコンテンツ情報送信スクリプト）つき HTML を受けたクライアント計算機の Web ブラウザでは、この不正スクリプトすなわち漏洩先サイトへのコンテンツ情報送信スクリプトを実行してしまう。

（7）この結果、クライアント計算機から漏洩先サイトへのコンテンツ情報の不正送信がなされてしまう。例えば、このコンテンツ情報に、データベース 101 からの秘密情報が含まれていれば、秘密情報が漏洩してしまうことになる。

（8）このようにして、漏洩先サイト（1c）は、攻撃したクライアント計算機やそのユーザ固有の情報を不正に取得することができる。

（9）これによって、漏洩先サイトは、例えば、攻撃したクライアント計算機になりまして、先の Web サーバへアクセスすることができたり、他の入手した情報を流用することができる。

【0091】

次に、図 11 を参照しながら、従来の通信システムにおけるクロスサイトスクリプティング脆弱性による form 送信先変更による form 入力詐取について説明する。

【0092】

クロスサイトスクリプティングでは、ユーザが閲覧する Web ページに不正なスクリプ

トプログラムを混入させてユーザのWebブラウザで実行させることで、form送信先を変更することによってform入力を詐取するなどの不正が行われ得る。

【0093】

ここで、図11のWebサーバ(1a)は、脆弱性を持つものとする(なお、このWebサーバ自体は正当なものである)。

【0094】

(1) まず、攻撃者がクライアント計算機へ不正コンテンツを送付する。これは、例えば、広告メールや、掲示板での誘導など、種々の方法で行われる。

(2) クライアント計算機のWebブラウザが、この不正コンテンツをレンダリングする。

(3) そして、クライアント計算機からWebサーバへ、例えばform送信先の不正な変更スクリプトのもととなるデータ等の不正データを含むGETリクエストを送出してしまふ。

(4) このGETリクエストを受けたWebサーバは、誤った出力処理をしてしまふ。

(5) この結果、不正スクリプト(漏洩先サイトへのform送信先の不正な変更スクリプト)つきHTMLを送付してしまふ。

(6) クライアント計算機のWebブラウザでは、formを正常に表示する。

(7) ユーザはWebブラウザに表示されたformに情報を入力し、送信操作を行う。

(8) 送信操作によって、クライアント計算機のWebブラウザでは、この不正スクリプトすなわち漏洩先サイトへのform送信先変更スクリプトを実行し、その後情報を送信してしまふ。

(9) この結果、クライアント計算機から漏洩先サイトへのform入力情報の不正送信がなされてしまふ。

(10) このようにして、漏洩先サイト(1c)は、ユーザ固有の情報を不正に取得することができる。

(11) これによって、漏洩先サイトは、例えば、入手したユーザ固有の情報を流用することができる。

【0095】

次に、図12を参照しながら、従来の通信システムにおけるクロスサイトスクリプティング脆弱性によるリダイレクトを用いた偽formの表示による入力詐取について説明する。

【0096】

クロスサイトスクリプティングでは、ユーザが閲覧するWebページに不正なスクリプトプログラムを混入させてユーザのWebブラウザで実行させることで、外部の偽formを表示することによってform入力情報を詐取するなどの不正が行われ得る。

【0097】

ここで、図12のWebサーバ(1a)は、脆弱性を持つものとする(なお、このWebサーバ自体は正当なものである)。

【0098】

(1) まず、攻撃者がクライアント計算機へ不正コンテンツを送付する。これは、例えば、広告メールや、掲示板での誘導など、種々の方法で行われる。

(2) クライアント計算機のWebブラウザが、この不正コンテンツをレンダリングする。

(3) そして、クライアント計算機からWebサーバへ、例えば外部偽form表示スクリプトのもととなるデータ等の不正データを含むGETリクエストを送出してしまふ。

(4) このGETリクエストを受けたWebサーバは、誤った出力処理をしてしまふ。

(5) この結果、不正スクリプト（外部偽 f o r m出力スクリプト）つきHTMLを送付してしまう。

(6) クライアント計算機のWebブラウザでは、リダイレクト不正スクリプトを実行する。

(7) クライアント計算機のWebブラウザでは、不正リダイレクト先のリクエストを指示されたサーバ、ここでは漏洩先サイトへ送信する。

(8) 漏洩先サイトは f o r mを含んだHTMLコンテンツを送付する。f o r mの送信先は漏洩先サイトとなっている。

(9) クライアント計算機のWebブラウザでは漏洩先サイトから送付された f o r m、すなわち偽 f o r mを正規のコンテンツと一体に表示する。

(10) ユーザはWebブラウザに表示された偽 f o r mに情報を入力し、送信操作を行う。

(11) クライアント計算機のWebブラウザは、ユーザの送信操作によって偽 f o r mに入力された情報を漏洩先サイトへ送信してしまう。

この結果、クライアント計算機から漏洩先サイトへの f o r m入力情報の不正送信がなされてしまう。

(12) このようにして、漏洩先サイト（1c）は、ユーザ固有の情報を不正に取得することができる。

(13) これによって、漏洩先サイトは、例えば、入手したユーザ固有の情報を流用することができる。

【0099】

さらに、図13を参照しながら、従来の通信システムにおけるクロスサイトスクリプティング脆弱性による外部偽 f o r m表示による f o r m入力詐取について説明する。

【0100】

クロスサイトスクリプティングでは、ユーザが閲覧するWebページに不正なスクリプトプログラムを混入させてユーザのWebブラウザで実行させることで、外部の偽 f o r mを表示することによって f o r m入力情報を詐取するなどの不正が行われ得る。

【0101】

ここで、図13のWebサーバ（1a）は、脆弱性を持つものとする（なお、このWebサーバ自体は正当なものである）。

【0102】

(1) まず、攻撃者がクライアント計算機へ不正コンテンツを送付する。これは、例えば、広告メールや、掲示板での誘導など、種々の方法で行われる。

(2) クライアント計算機のWebブラウザが、この不正コンテンツをレンダリングする。

(3) そして、クライアント計算機からWebサーバへ、例えば外部偽 f o r m表示スクリプトのもととなるデータ等の不正データを含むGETリクエストを送出してしまう。

(4) このGETリクエストを受けたWebサーバは、誤った出力処理をしてしまう。

(5) この結果、不正スクリプト（外部偽 f o r m出力スクリプト）つきHTMLを送付してしまう。

(6) クライアント計算機のWebブラウザでは、不正スクリプトを実行し、不正に挿入された i f r a m eタグの処理を行う。

(7) クライアント計算機のWebブラウザでは i f r a m eタグの表示のため、i f r a m eタグの中身のリクエストを指示されたサーバ、ここでは漏洩先サイトへ送信する。

(8) 漏洩先サイトは f o r mを含んだHTMLコンテンツを送付する。f o r mの送信先は漏洩先サイトとなっている。

(9) クライアント計算機のWebブラウザでは漏洩先サイトから送付された f o r m

、すなわち偽 f o r m を正規のコンテンツと一体に表示する。

(10) ユーザは W e b ブラウザに表示された偽 f o r m に情報を入力し、送信操作を行う。

(11) クライアント計算機の W e b ブラウザは、ユーザの送信操作によって偽 f o r m に入力された情報を漏洩先サイトへ送信してしまう。

この結果、クライアント計算機から漏洩先サイトへの f o r m 入力情報の不正送信がなされてしまう。

(12) このようにして、漏洩先サイト (1 c) は、ユーザ固有の情報を不正に取得することができる。

(13) これによって、漏洩先サイトは、例えば、入手したユーザ固有の情報を流用することができる。

【0103】

次に、図 1 4 を参照しながら、従来の通信システムにおけるクロスサイトスクリプティング脆弱性による偽 f o r m の追加による f o r m 入力詐取について説明する。

【0104】

クロスサイトスクリプティングでは、ユーザが閲覧する W e b ページに不正なスクリプトプログラムを混入させてユーザの W e b ブラウザで実行させることで、f o r m 送信先を変更することによって f o r m 入力を詐取するなどの不正が行われ得る。

【0105】

ここで、図 1 4 の W e b サーバ (1 a) は、脆弱性を持つものとする（なお、この W e b サーバ自体は正当なものである）。

【0106】

(1) まず、攻撃者がクライアント計算機へ不正コンテンツを送付する。これは、例えば、広告メールや、掲示板での誘導など、種々の方法で行われる。

(2) クライアント計算機の W e b ブラウザが、この不正コンテンツをレンダリングする。

(3) そして、クライアント計算機から W e b サーバへ、例えば外部偽 f o r m 表示スクリプトのもととなるデータ等の不正データを含む G E T リクエストを送出してしまう。

(4) この G E T リクエストを受けた W e b サーバは、誤った出力処理をしてしまう。

(5) この結果、不正スクリプト（外部偽 f o r m 出力スクリプト）つき H T M L を送付してしまう。

(6) クライアント計算機の W e b ブラウザでは、不正スクリプトを実行する。

(7) クライアント計算機の W e b ブラウザでは漏洩先サイトから送付された f o r m 、すなわち偽 f o r m を正規のコンテンツと一体に表示する。

(8) ユーザは W e b ブラウザに表示された偽 f o r m に情報を入力し、送信操作を行う。

(9) クライアント計算機の W e b ブラウザは、ユーザの送信操作によって偽 f o r m に入力された情報を漏洩先サイトへ送信してしまう。

この結果、クライアント計算機から漏洩先サイトへの f o r m 入力情報の不正送信がなされてしまう。

(10) このようにして、漏洩先サイト (1 c) は、ユーザ固有の情報を不正に取得することができる。

(11) これによって、漏洩先サイトは、例えば、入手したユーザ固有の情報を流用することができる。

【0107】

これに対して、本実施形態では、図 1 0、図 1 1、図 1 2、図 1 3、図 1 4 の W e b サーバとインターネットとの間に存在するプロキシサーバにおいて、図 1 0 の (5)、図 1 1 の (5)、図 1 2 の (5)、図 1 3 の (5)、図 1 4 の (5) の不正スクリプトつき H

TMLを遮断するようにし、これによって、クッキー情報等の漏洩を防止することができるようになっている。

【0108】

以下、本実施形態のより詳細な動作例について説明する。

【0109】

図7及び図15に、本実施形態のプロキシサーバ3の処理手順の一例を示す。

【0110】

なお、ここでは一例として、スクリプトとしてJavaScript及びVBScriptを対象とし、スクリプトを含む可能性のある文書としてHTML、XML及びCSSを対象とするものとする。また、前述のように、Webブラウザに格納される情報の一例としてクッキーを考えるものとする。

【0111】

まず、ステップS1～ステップS19、ステップS22は、基本的には、第1の実施形態で説明した通りである（図7及び図8参照）。

【0112】

ただし、図8では、ステップS14において、スクリプト検査部35が、スクリプトの構文解析および意味解析を行い、スクリプトで扱うオブジェクトの依存ツリーを作成した後に、ステップS15において、依存ツリー中でDocumentオブジェクトのCookieプロパティが参照されていなければ、ステップS20へ進んだが、図15では、次のようになる。すなわち、ステップS14の後、ステップS15-1において、依存ツリー中でDocumentオブジェクトが参照されていれば、ステップS15-2へ進み、参照されていなければ、ステップS33へ進み、ステップS15-2において、Cookieプロパティが参照されていれば、ステップS16へ進み、Cookieプロパティが参照されていなければ、ステップS31へ進む。

【0113】

さて、スクリプト検査部35では、さらに、Documentオブジェクトが参照されているケース（ステップS15-2、S16、S17でNoの場合）において、Documentオブジェクトが別コンテンツのURLやformのデータとされている場合（ステップS31）、それらのURLが送信許可判定部352において送信許可リスト3521の内容と合致するかどうか検査する（ステップS32）。オブジェクト依存ツリーにおける定数の畳み込みに関する処理や許可されない送信が含まれると判断された場合の処理は、クッキーの検査の場合と同一である（ステップS18、S19、S22）。また、ステップS31でNoの場合およびステップS32でNoの場合には、ステップS33に進む。

【0114】

スクリプト検査部35では、さらに、ステップS15-2、S31、S32でNoのケースにおいて、formのactionプロパティへの代入や変更などが行われている場合（ステップS33）、それらのURLが送信先許可判定部353において送信先許可リスト3531の内容と合致するかどうか検査する（ステップS34）。定数の畳み込みに関する処理や許可されない送信が含まれると判断された場合の処理はクッキーの検査の場合と同一である（ステップS18、S19、S22）。また、ステップS33でNoの場合およびステップS34でNoの場合には、ステップS35に進む。

【0115】

スクリプト検査部35では、さらに、ステップS33、S34でNoのケースにおいて、オブジェクトのlocationプロパティの変更が行われている場合（ステップS35）、およびiframeのsrcプロパティの変更が行われている場合（ステップS36）、それらのURLが要求先許可判定部354において要求先許可リスト3541の内容と合致するかどうか検査する（ステップS42）。定数の畳み込みに関する処理や許可されない送信が含まれると判断された場合の処理はクッキーの検査の場合と同一である（ステップS18、S19、S22）。

【0116】

また、スクリプト検査部35では、ステップS35でNoかつステップS36でNo、またはステップS42でNoのケースにおいて、Documentオブジェクトのwriteメソッドが呼び出されているかどうかを検査する(ステップS37)。Documentオブジェクトのwriteメソッドによって、Webブラウザによって解釈されるドキュメントが生成されるため、そのなかで外部コンテンツを表示するタグが含まれていれば偽formの表示につながり、またそのなかにスクリプトが含まれていれば実行される可能性があるためである。すなわち、Documentオブジェクトのwriteメソッドが呼び出される場合(ステップS37)には、スクリプトを部分的に実行する形で新しい文書を作成し(ステップS38)、文書の型に応じた構文解析を行い(ステップS39)、formが生成される場合(ステップS40)には、ステップS34に進んで、form送信先判定部353で検査を行い、iframeが生成される場合(ステップS41)には、ステップS42に進んで、外部コンテンツ要求先判定部354で検査を行い、それ以外の場合(ステップS41でNoの場合)は、文書解釈部34へ処理を渡してスクリプトが含まれるかどうか検査するところ(ステップS13)に戻る。なお、ステップS37でNoの場合には、Webサーバ1から受信したHTTPレスポンスを、そのままWebブラウザに送信する形で、返信する(ステップS22)。

【0117】

以上のような検査をへてスクリプトが不正な情報漏洩を行わないと判断できる場合に、Webサーバから受信したHTTPレスポンスを、そのままWebブラウザに送信する形で、返信する。

【0118】

このように本実施形態によれば、秘匿すべき情報の漏洩を防止することができる。

【0119】

なお、上記では、当該Webコンテンツについて送信が許可されないと判断された場合に、当該WebコンテンツのWebブラウザ(クライアント計算機2)への送出を禁止するとともに、通知メッセージの送信や、エラーメッセージの送信を行ったが、通知メッセージの送信とエラーメッセージの送信の一方又は両方を行わない構成も可能である(ログを保存しない構成も可能である)。

【0120】

なお、上記では、送信許可判定部351、送信先判定部352、送信先判定部353、要求先判定部354は、それぞれ、送信先一覧をURLとして保持した送信許可リスト3511を送信許可規則とし照合する場合、送信先一覧をURLとして保持した送信許可リスト3521、送信先一覧をURLとして保持した送信先許可リスト3531、要求先一覧をURLとして保持した要求先許可リスト3541を例にとって説明しているが、その代わりに、許可されるURLを正規表現の記述として保有し、個々のURLと照合して全てのURLが正規表現と一致する場合にのみ許可の結果を返すようにしてもよい、両者を併用してもよい。

【0121】

ところで、第2の実施形態は、クッキー送信許可判定部351と情報送信許可判定部352とフォーム送信先許可判定部353と外部コンテンツ要求先許可判定部354をすべて備え、第1の実施形態は、それらのうちクッキー(Cookie)送信許可判定部351のみを備えるものであったが、情報送信許可判定部352とフォーム(form)送信先許可判定部353と外部コンテンツ要求先許可判定部354とのうちのいずれか1つのみを備える形態や、クッキー送信許可判定部351と情報送信許可判定部352とフォーム送信先許可判定部353と外部コンテンツ要求先許可判定部354のうちのいずれか2つまたは3つを備える形態も可能である。

【0122】

また、第1の実施形態若しくは第2の実施形態又は上記のようなそれ以外の各種形態において、本プロキシサーバ(通信中継装置)は、1つの装置(例えば、計算機)で構成し

てもよいし、複数の装置（例えば、計算機）で構成してもよい。

【0123】

後者の場合に、例えば、本プロキシサーバを構成する計算機から、送信許可判定部のみを独立させて、これをもう一つの計算機で構成するようにしてもよい。この場合、プロキシサーバ本体たる計算機と各許可判定部たる計算機とは、例えば、専用線で接続してもよいし、インターネットを介して接続するようにしてもよい（後者の場合には、暗号通信等によりセキュリティを確保するのが好ましい）。

【0124】

また、上記の場合に、プロキシサーバ本体たる計算機と許可判定部たる計算機との対応関係については、1つの許可判定部たる計算機を唯一のプロキシサーバ本体たる計算機のみが使用可能とする構成と、1つの許可判定部たる計算機を複数のプロキシサーバ本体たる計算機が使用可能とする構成とが可能である。

【0125】

また、これまでの各種形態では、本プロキシサーバ（通信中継装置）とWebサーバとを別々の装置（例えば、計算機）で構成するものとして説明したが、例えば、本プロキシサーバ（通信中継装置）の不正コンテンツを遮断する機能に相当する部分（例えば、図2や図9のコンテンツ分類部33、文書解釈部34、スクリプト検査部35、及びネットワーク側通信インタフェース31の機能のうちのエラーメッセージや通知メッセージ等を生成し送信する機能）の部分、Webサーバに含まれる機能拡張モジュールとして実現することも可能である。また、この場合にも、上記のように、Webサーバ本体と送信許可判定部とを別々の計算機で実現するような構成も可能である。

【0126】

また、これまでの各種形態では、ネットワークとしてインターネットを取り上げたが、もちろん、他のネットワークでも適用可能である。

【0127】

また、これまでの各種形態では、スクリプトとしてJavaScript及びVBScriptを対象とし、スクリプトを含む可能性のある文書としてHTML、XML及びCSSを対象とする場合を取り上げたが、もちろん、当該ネットワークで使用されるスクリプトあるいは不正に使用される可能性のあるスクリプトなど適宜の基準で対象とするスクリプトを選択して構わない。スクリプトを含む可能性のある文書についても同様である。また、新たなスクリプトや、スクリプトを含む可能性のある新たな文書が発生した場合には、それらを新たに対象として追加すればよい。

【0128】

なお、以上の各機能は、ソフトウェアとして記述し適当な機構をもったコンピュータに処理させても実現可能である。

また、本実施形態は、コンピュータに所定の手段を実行させるための、あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるためのプログラムとして実施することもできる。加えて該プログラムを記録したコンピュータ読取り可能な記録媒体として実施することもできる。

【0129】

なお、本発明は上記実施形態そのままに限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で構成要素を変形して具体化できる。また、上記実施形態に開示されている複数の構成要素の適宜な組み合わせにより、種々の発明を形成できる。例えば、実施形態に示される全構成要素から幾つかの構成要素を削除してもよい。さらに、異なる実施形態にわたる構成要素を適宜組み合わせてもよい。

【図面の簡単な説明】

【0130】

【図1】本発明の第1の実施形態に係る通信システムの構成例を示す図

【図2】同実施形態に係る通信中継装置の構成例を示す図

【図3】送信許可リストの一例を示す図

【図 4】クッキーの典型的利用形態について説明するための図

【図 5】提携サイトへのクッキー送信例について説明するための図

【図 6】クロスサイトスクリプティング脆弱性によるクッキー漏洩及び同実施形態に係る通信中継装置による不正コンテンツの遮断によるクッキー漏洩の回避について説明するための図

【図 7】本発明の第 1 及び第 2 の実施形態に係る通信制御装置の処理手順の一例を示すフローチャート

【図 8】本発明の第 1 の実施形態に係る通信制御装置の処理手順の一例を示すフローチャート

【図 9】本発明の第 2 の実施形態に係る通信中継装置の構成例を示す図

【図 1 0】クロスサイトスクリプティング脆弱性によるコンテンツ情報漏洩及び同実施形態に係る通信中継装置による不正コンテンツの遮断によるコンテンツ漏洩の回避について説明するための図

【図 1 1】クロスサイトスクリプティング脆弱性による f o r m 送信先変更による情報詐取及び同実施形態に係る通信中継装置による不正コンテンツの遮断による情報詐取の回避について説明するための図

【図 1 2】クロスサイトスクリプティング脆弱性によるリダイレクトを用いた偽 f o r m の表示による入力詐取及び同実施形態に係る通信中継装置による不正コンテンツの遮断による入力詐取の回避について説明するための図

【図 1 3】クロスサイトスクリプティング脆弱性による偽 f o r m 表示による情報詐取及び同実施形態に係る通信中継装置による不正コンテンツの遮断による情報詐取の回避について説明するための図

【図 1 4】クロスサイトスクリプティング脆弱性による偽 f o r m の追加による f o r m 入力詐取及び同実施形態に係る通信中継装置による不正コンテンツの遮断による情報詐取の回避について説明するための図

【図 1 5】同実施形態に係る通信制御装置の処理手順の一例を示すフローチャート

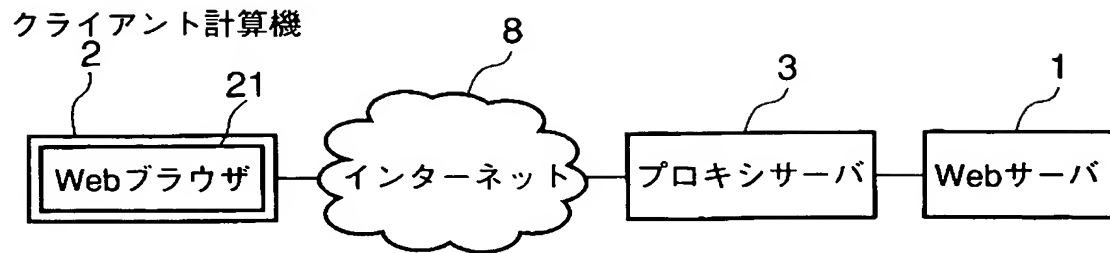
【符号の説明】

【 0 1 3 1 】

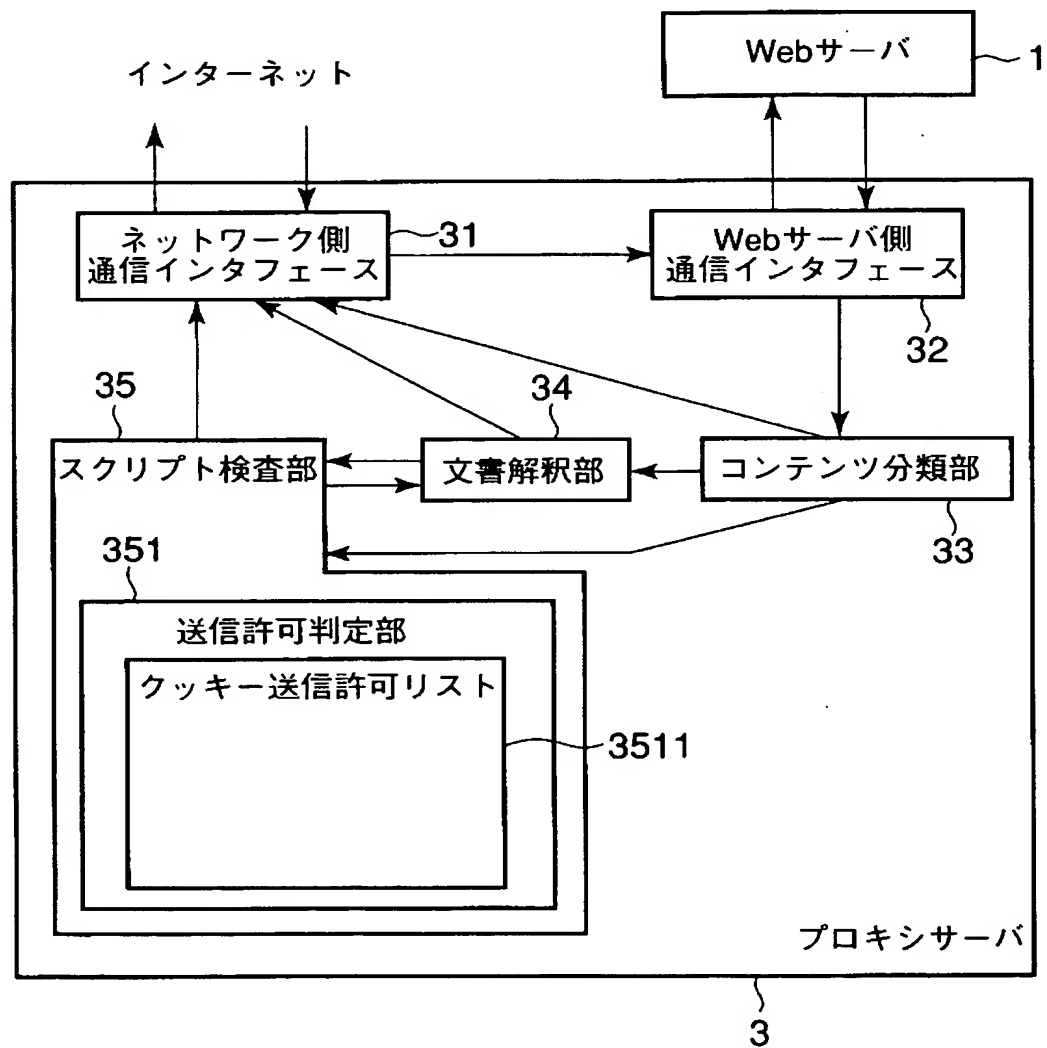
1…We b サーバ、2…通信中継装置、3…クライアント計算機、8…インターネット、2 1…We b ブラウザ、3 1…ネットワーク側通信インタフェース、3 2…サーバ側通信インタフェース、3 3…コンテンツ分類部、3 4…文書解釈部、3 5…スクリプト検査部、3 5 1…送信許可判定部、3 5 1 1…送信許可リスト

【書類名】図面

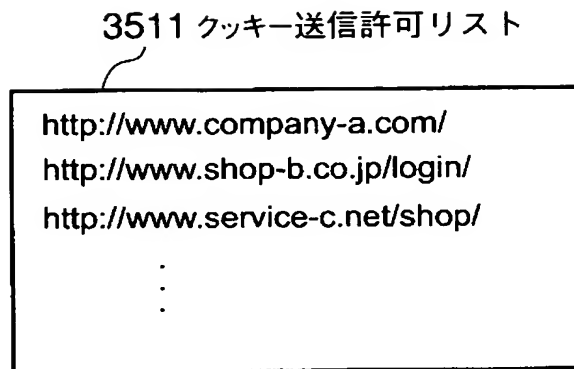
【図 1】



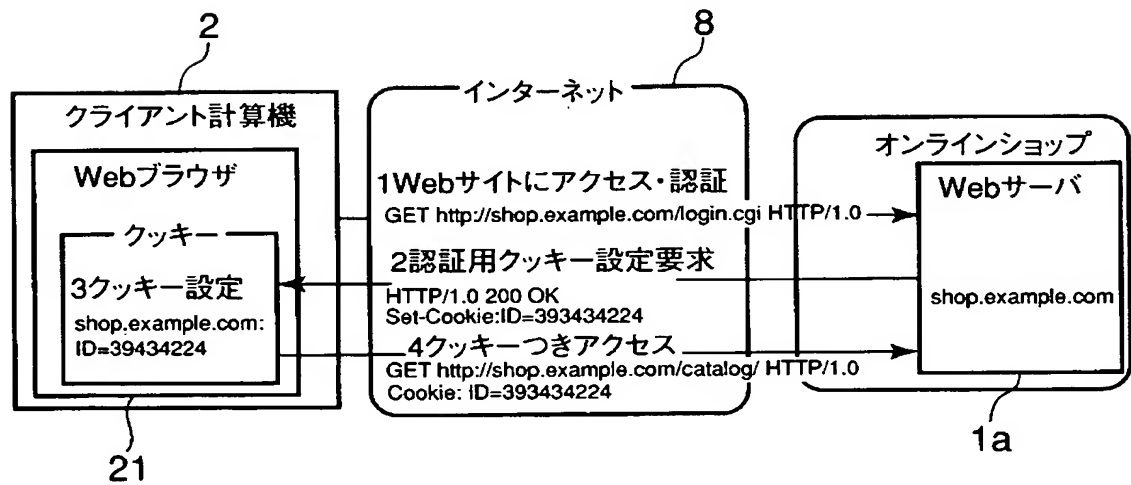
【図 2】



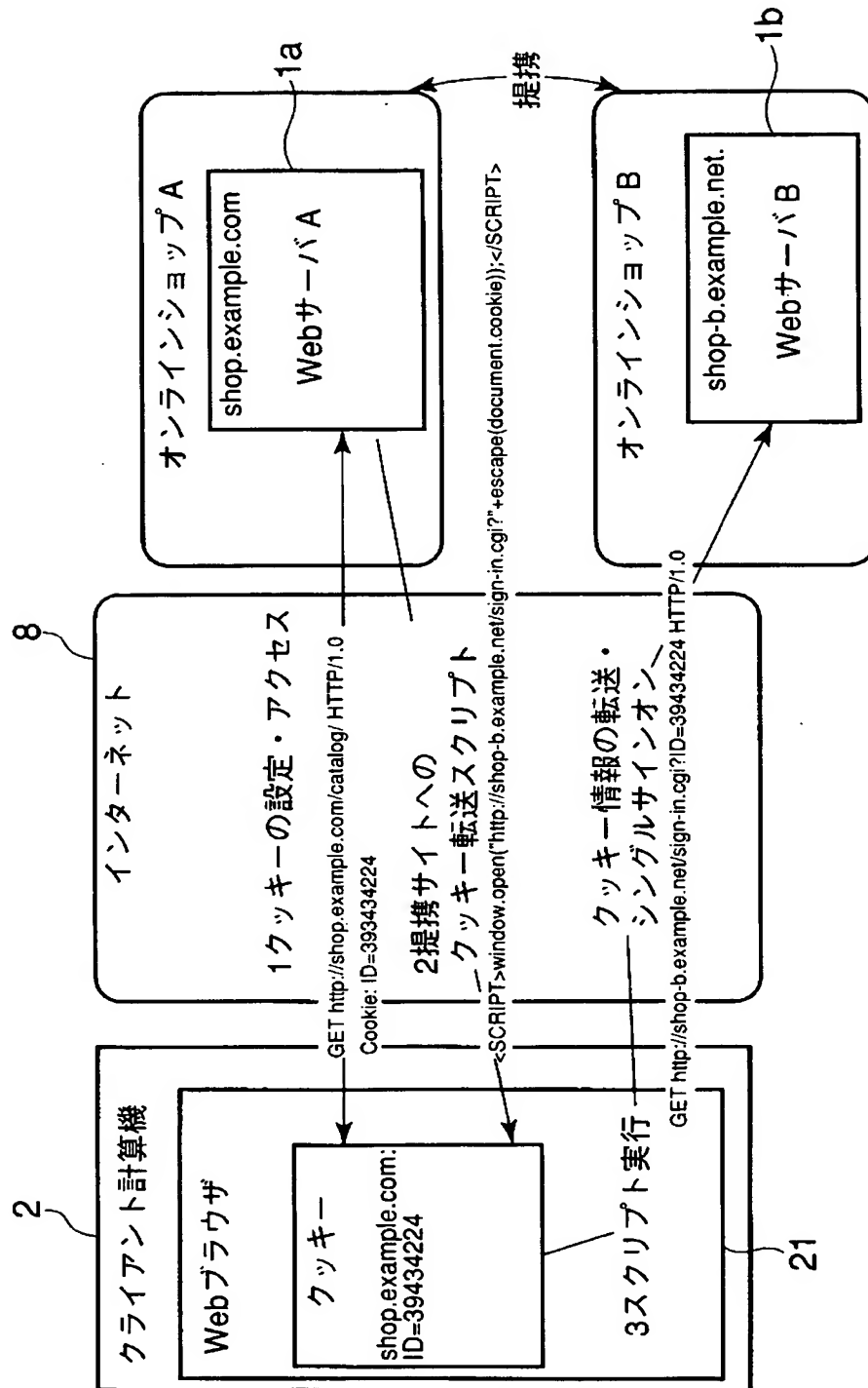
【図 3】



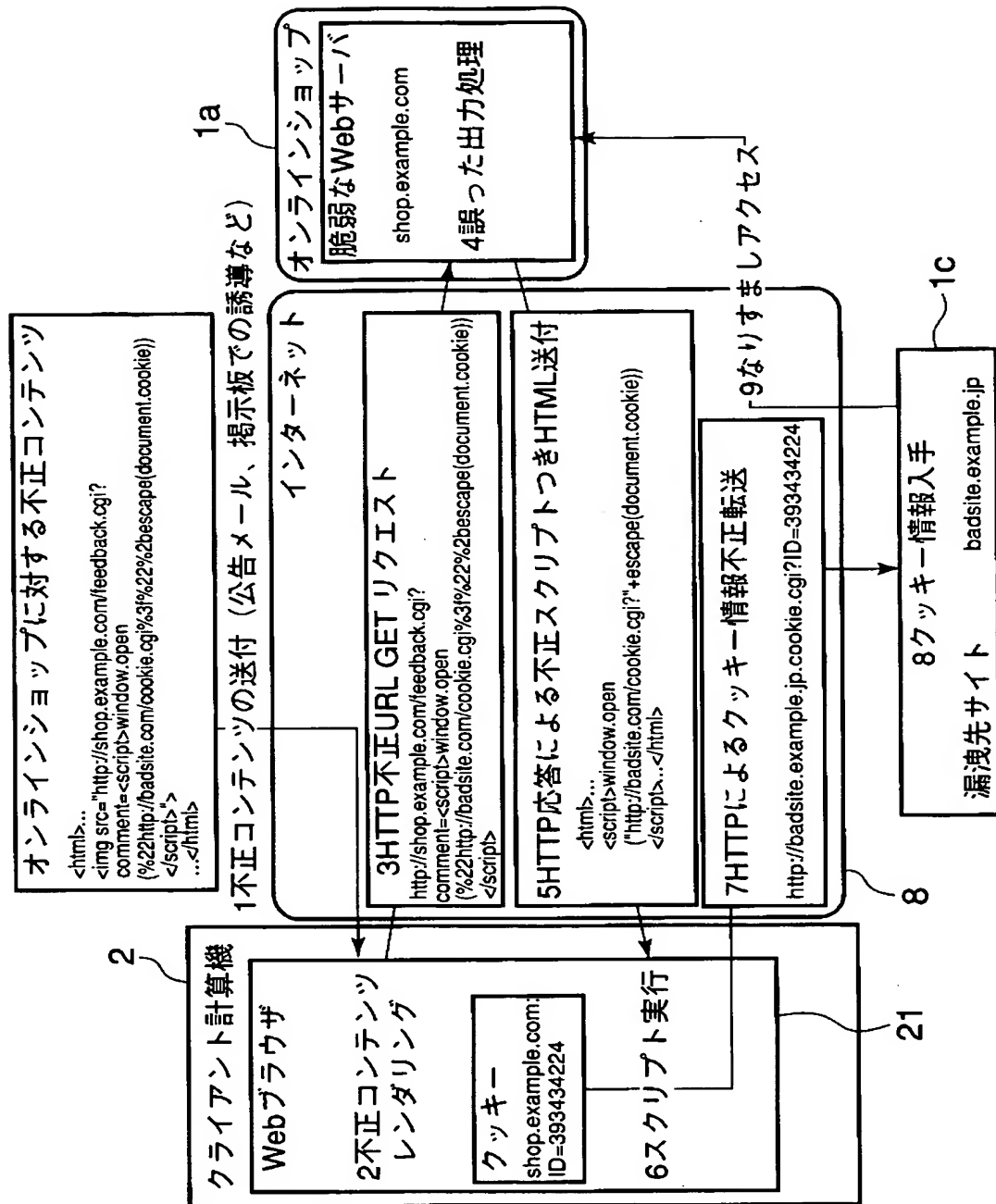
【図 4】



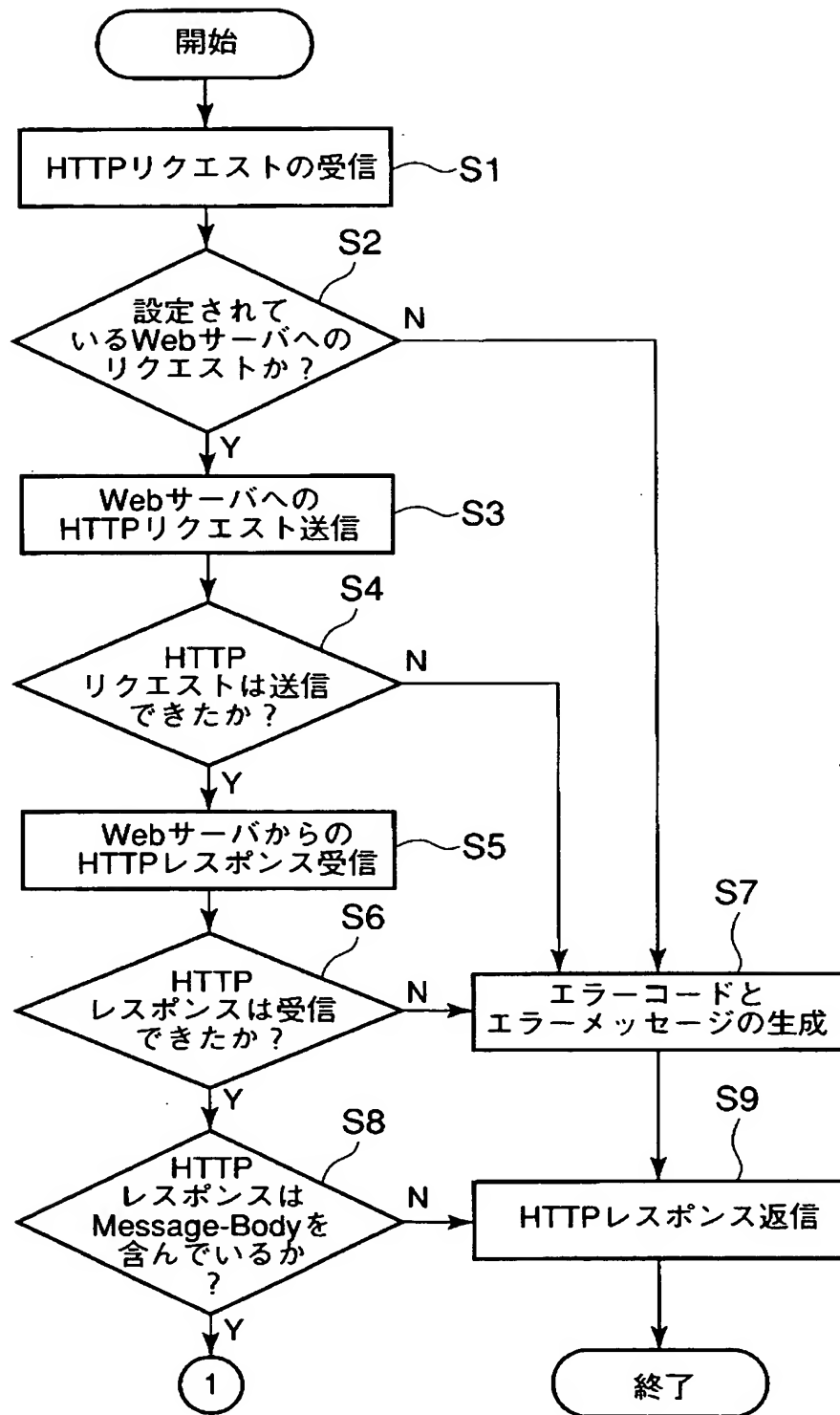
【図 5】



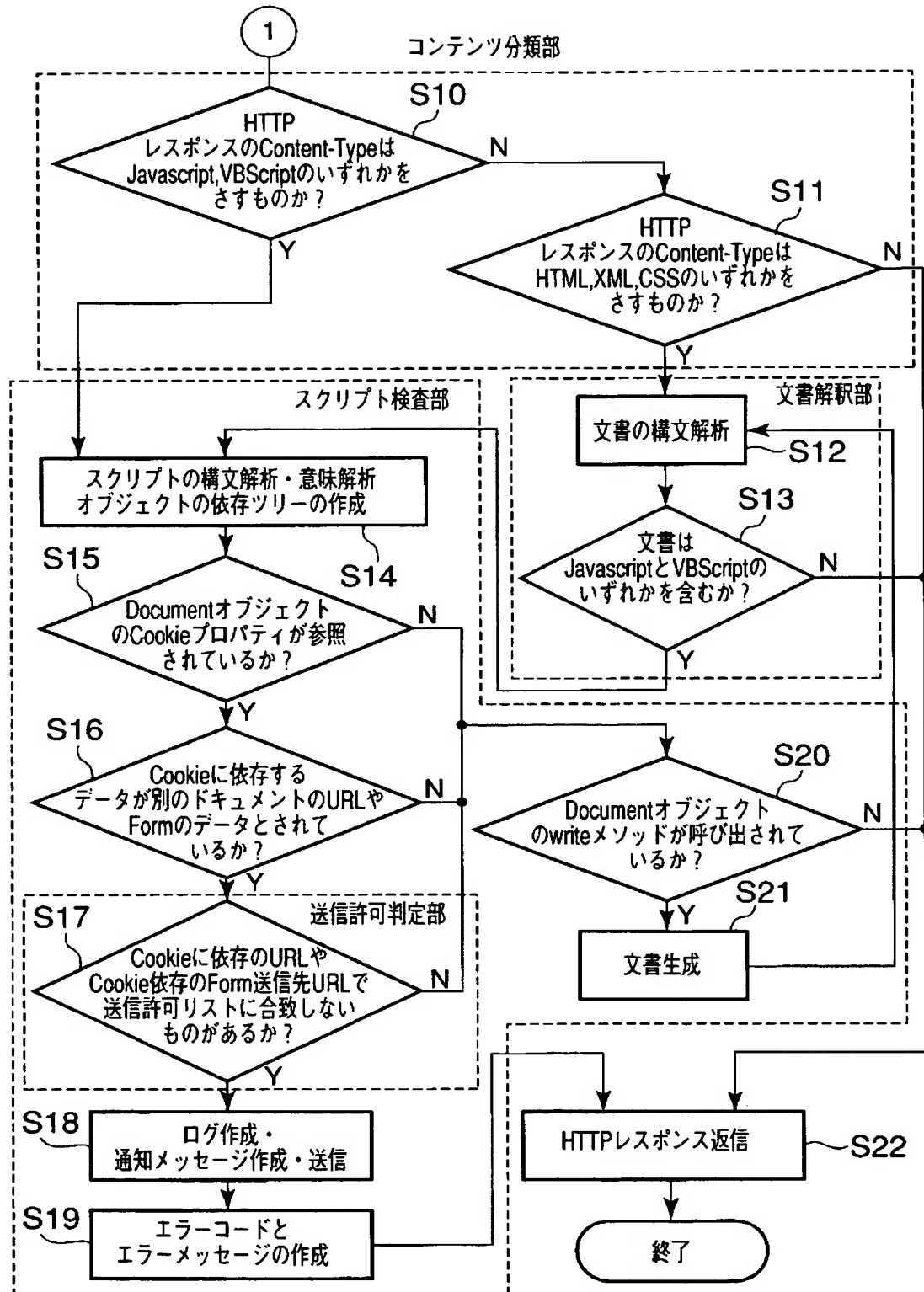
【図6】



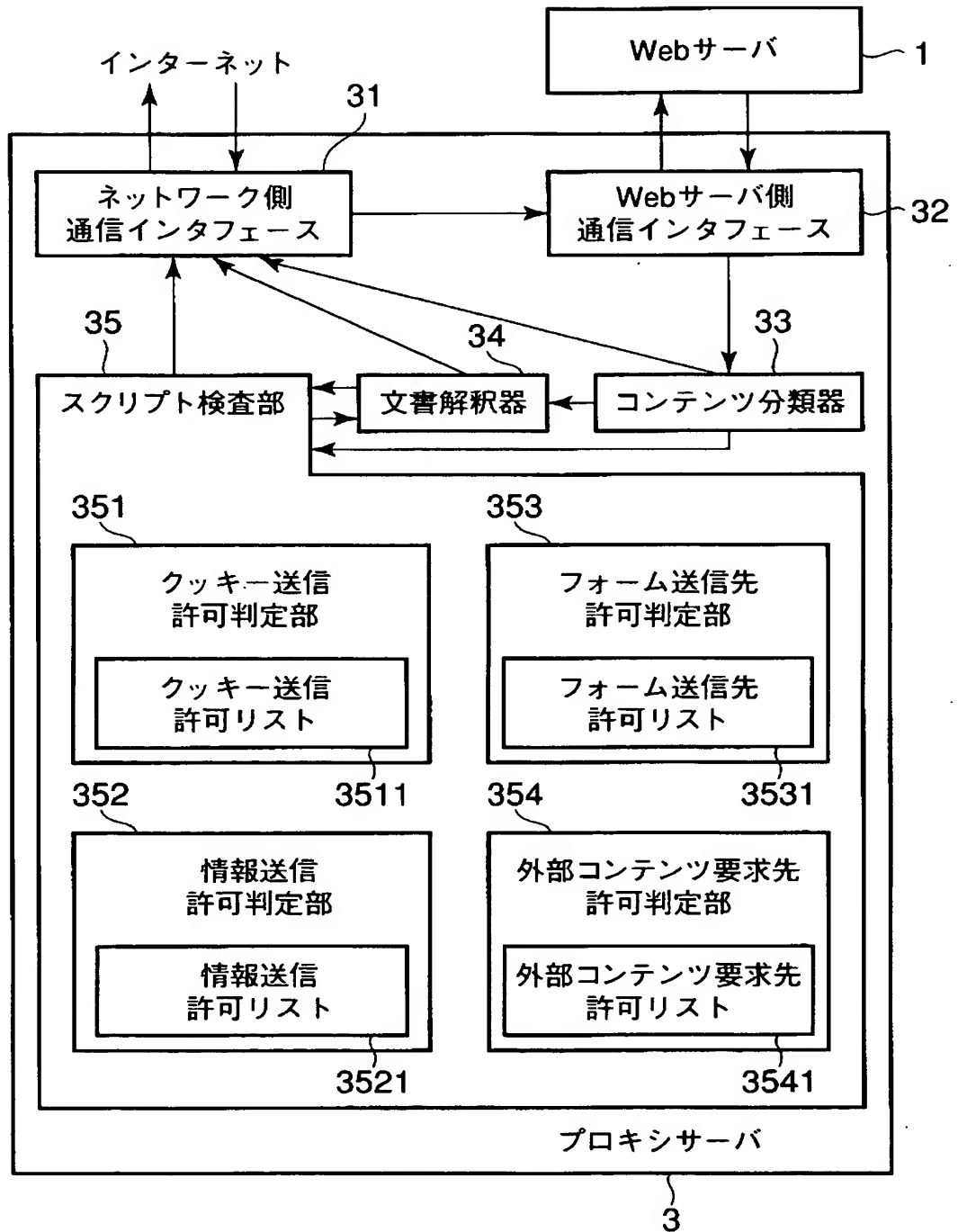
【図 7】



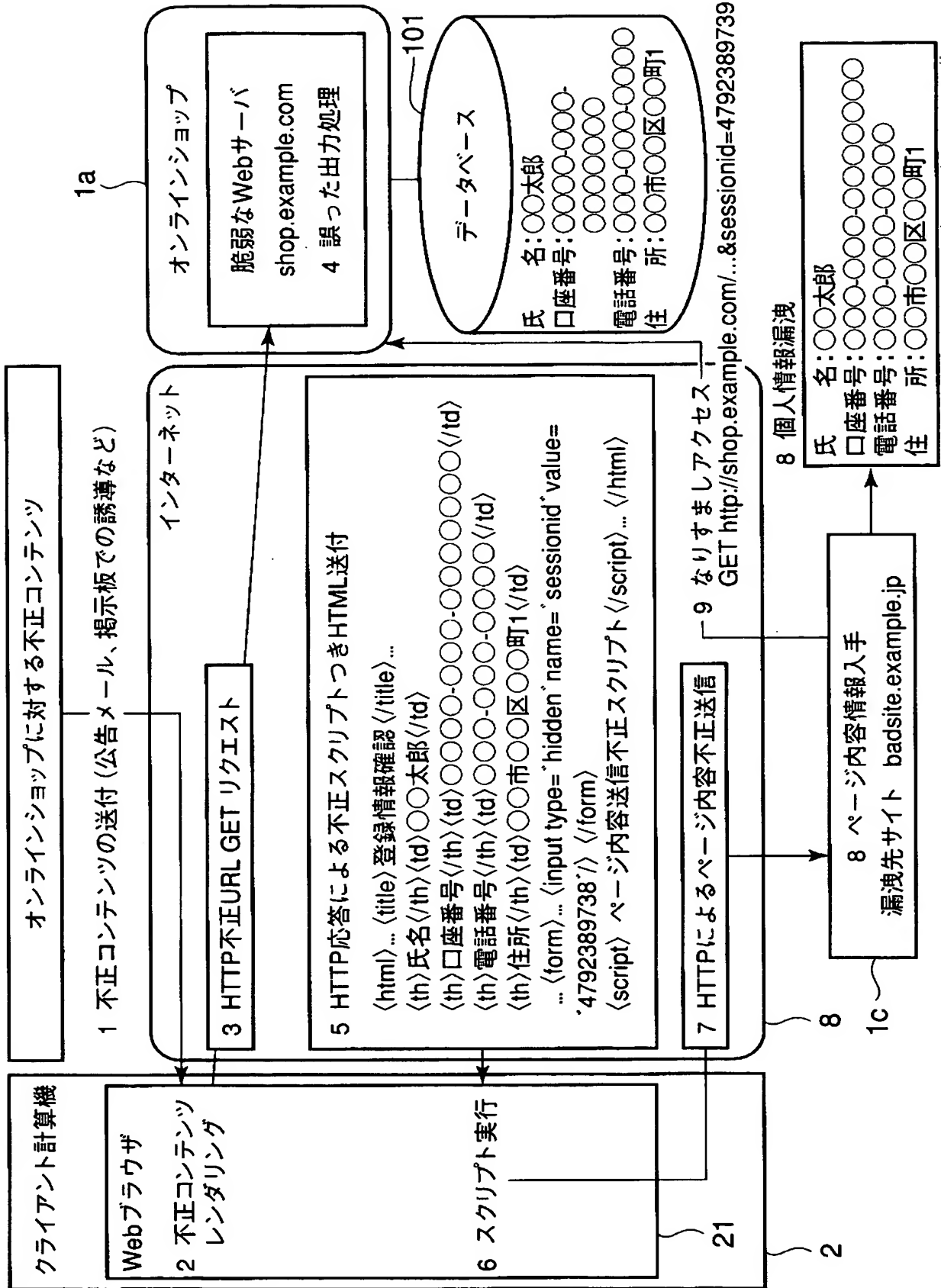
【図 8】



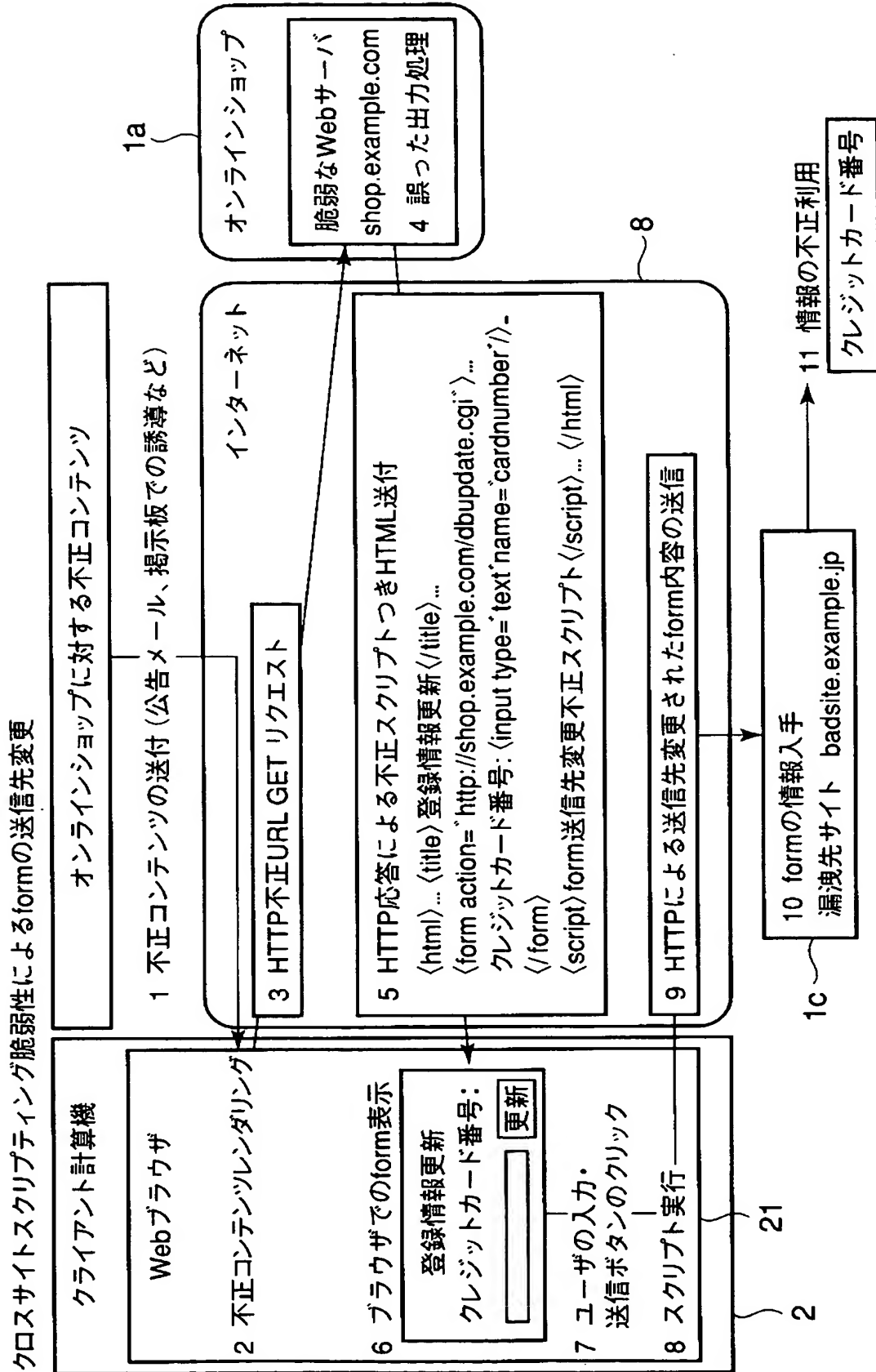
【図 9】



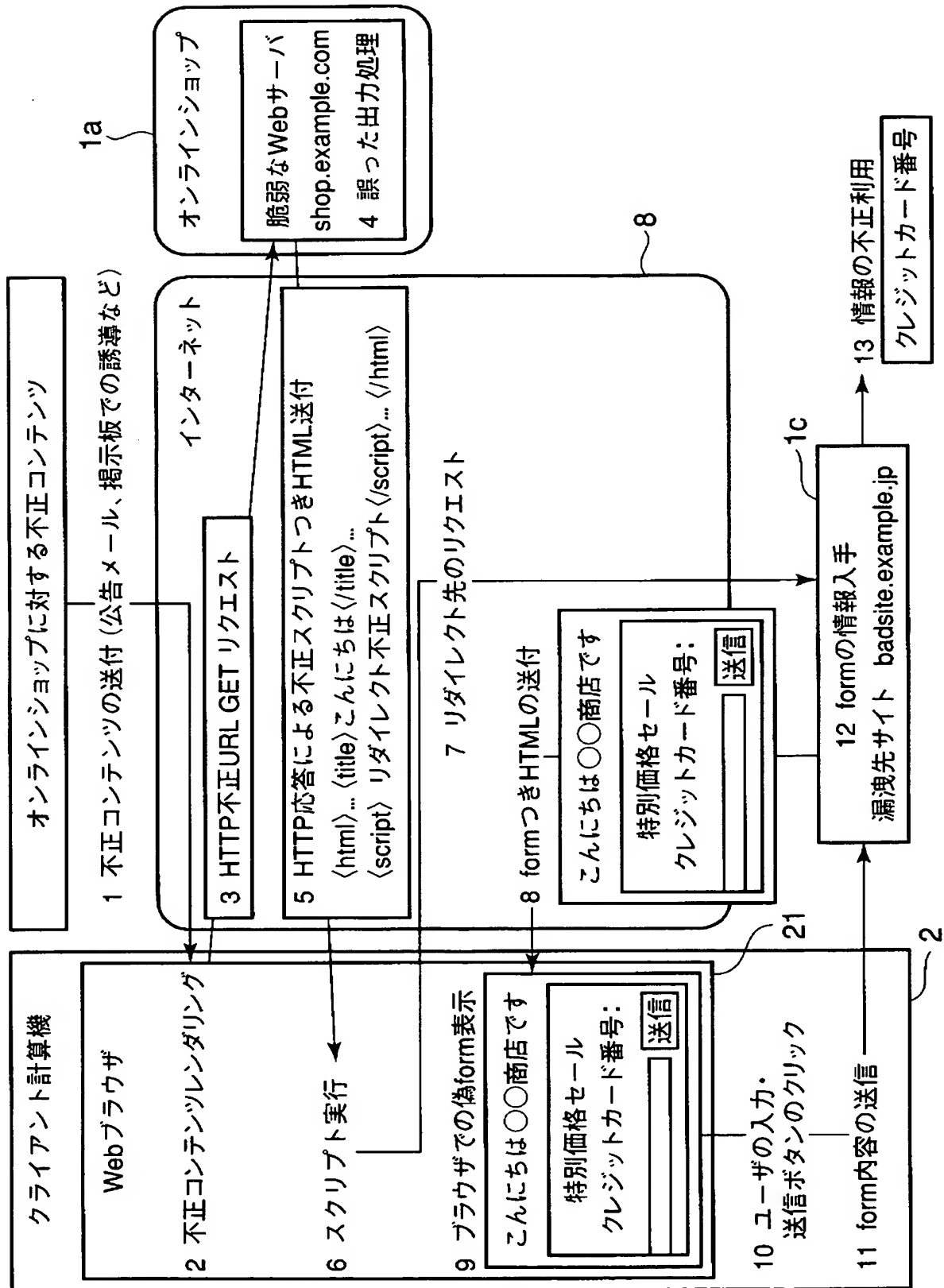
【図 10】



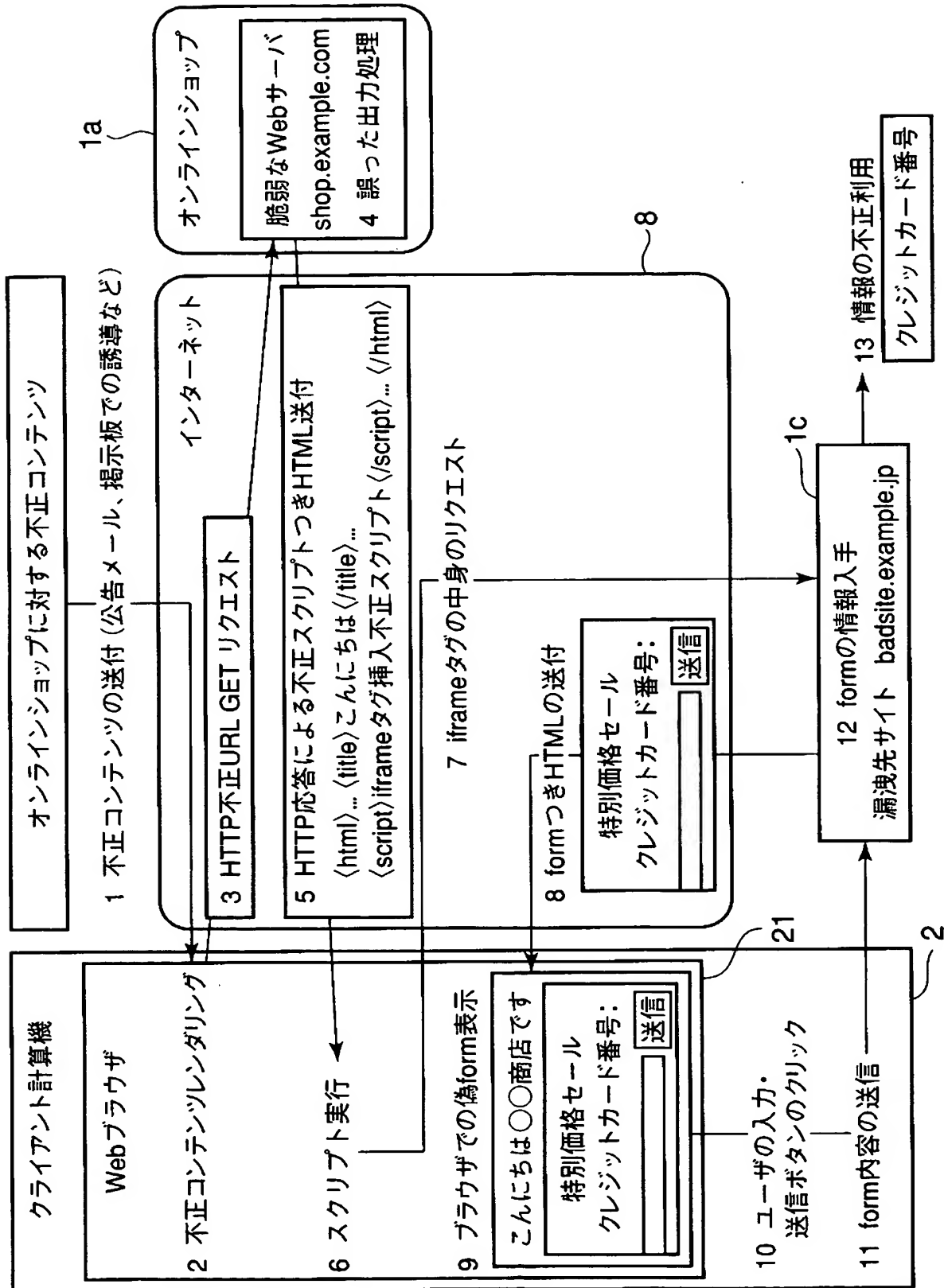
【図 11】



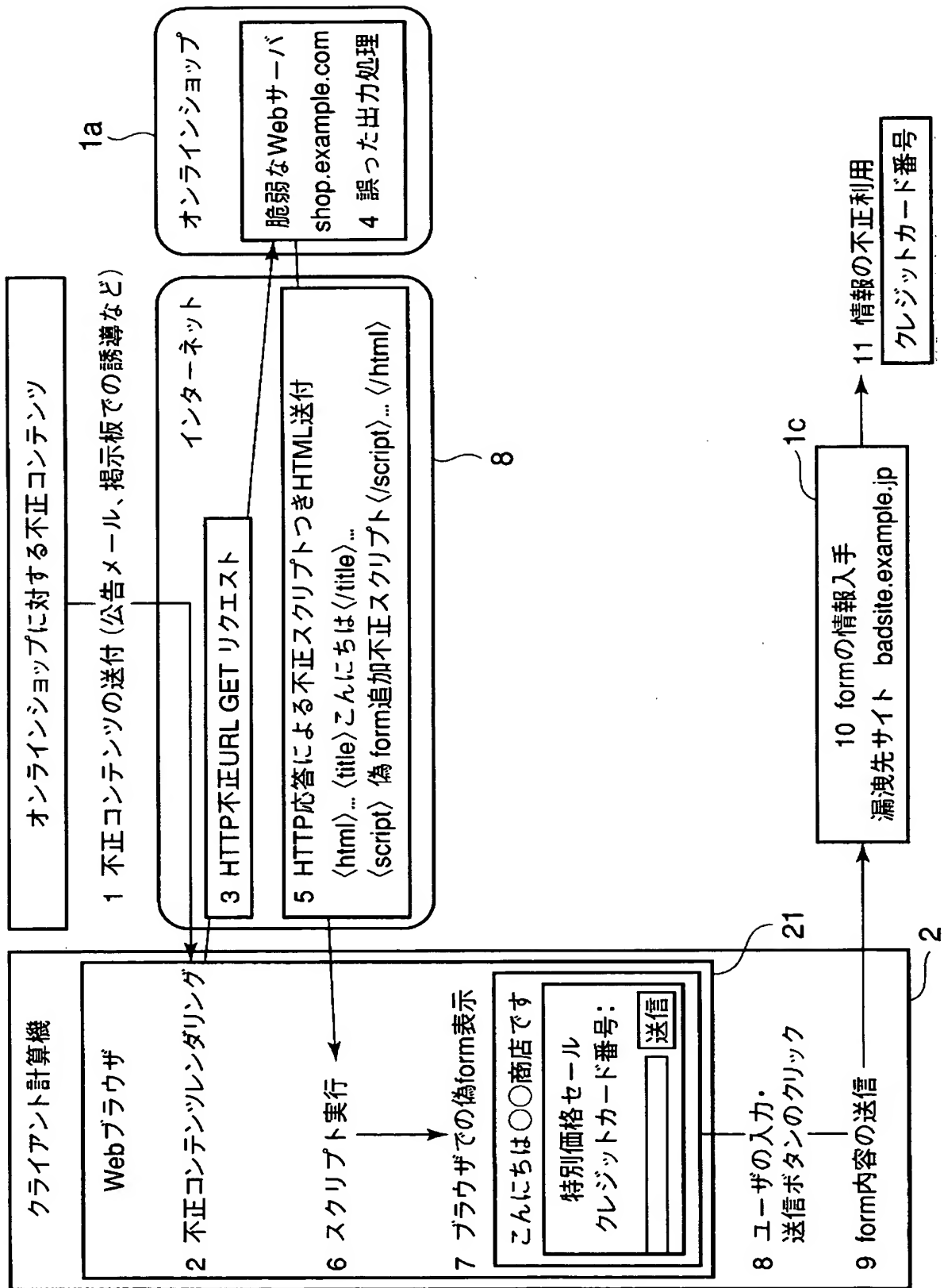
【図12】



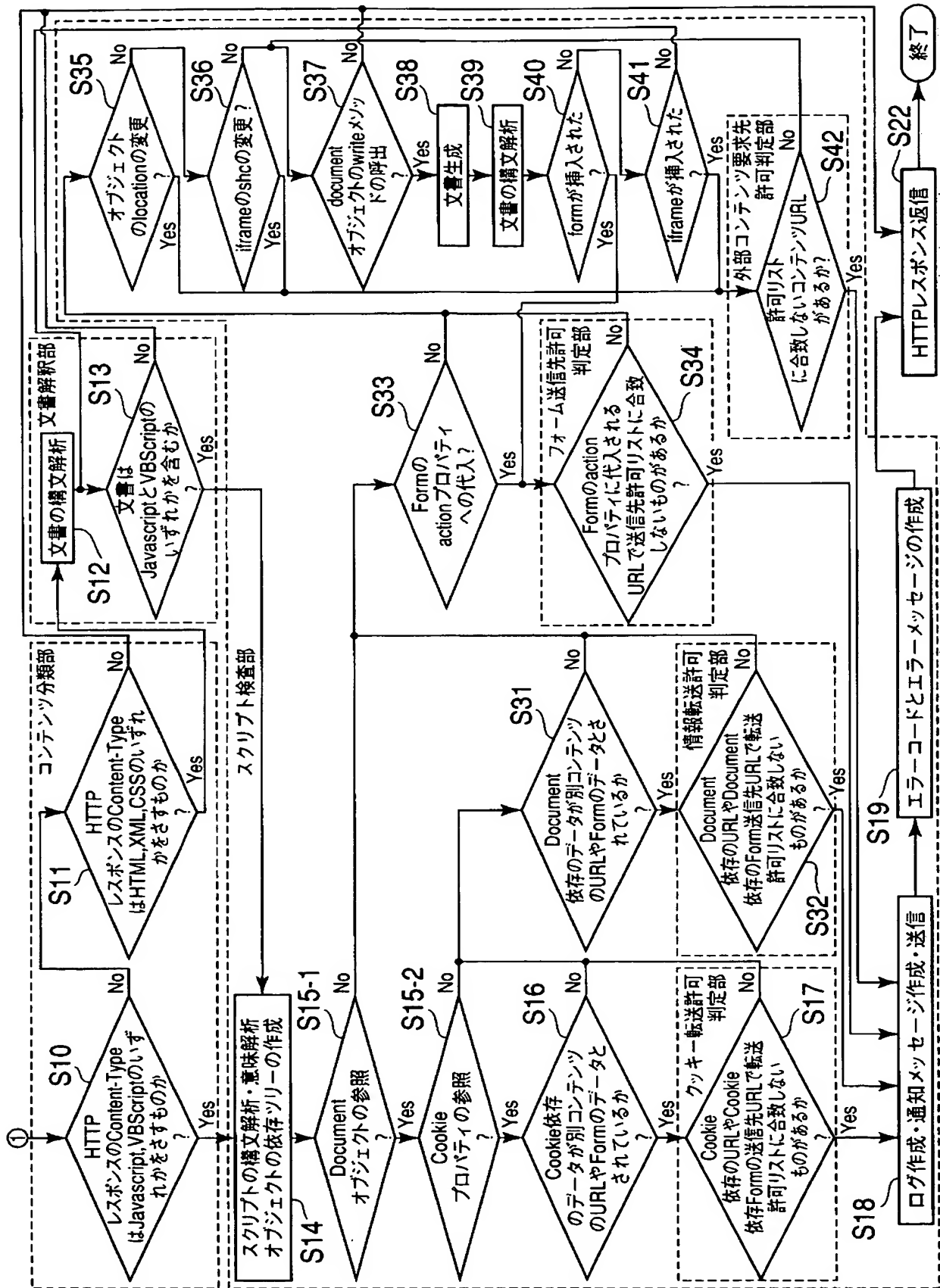
【図 13】



【図 14】



【図 15】



【書類名】 要約書**【要約】**

【課題】 サーバからクライアントに転送されるコンテンツ中に含まれる不正スクリプトによりクライアントに格納される情報が漏洩されること防止することのできる通信中継装置を提供すること。

【解決手段】 プロキシサーバ3は、Webサーバ1からWebブラウザ21へ転送されるコンテンツを受信すると、このコンテンツから、Webブラウザ21に格納されているクッキー情報をクライアント計算機2から外部の送信先へ向けて送出させる機能を有するスクリプトプログラムを抽出する。そのようなスクリプトプログラムが受信された場合、このコンテンツをクライアント計算機2へ送信してよいかどうかについての許否を判断し、送信が許可されたときにのみ、このコンテンツをクライアント計算機2へ送信する。

【選択図】 図1

認定・付加情報

特許出願の番号	特願 2003-400724
受付番号	50301971418
書類名	特許願
担当官	第八担当上席 0097
作成日	平成 15 年 12 月 3 日

< 認定情報・付加情報 >

【特許出願人】

【識別番号】	000003078
【住所又は居所】	東京都港区芝浦一丁目 1 番 1 号
【氏名又は名称】	株式会社東芝

【代理人】

申請人	
【識別番号】	100058479
【住所又は居所】	東京都千代田区霞が関 3 丁目 7 番 2 号 鈴榮特許 綜合法律事務所内
【氏名又は名称】	鈴江 武彦

【選任した代理人】

【識別番号】	100091351
【住所又は居所】	東京都千代田区霞が関 3 丁目 7 番 2 号 鈴榮特許 綜合法律事務所内
【氏名又は名称】	河野 哲

【選任した代理人】

【識別番号】	100088683
【住所又は居所】	東京都千代田区霞が関 3 丁目 7 番 2 号 鈴榮特許 綜合法律事務所内
【氏名又は名称】	中村 誠

【選任した代理人】

【識別番号】	100108855
【住所又は居所】	東京都千代田区霞が関 3 丁目 7 番 2 号 鈴榮特許 綜合法律事務所内
【氏名又は名称】	蔵田 昌俊

【選任した代理人】

【識別番号】	100084618
【住所又は居所】	東京都千代田区霞が関 3 丁目 7 番 2 号 鈴榮特許 綜合法律事務所内
【氏名又は名称】	村松 貞男

【選任した代理人】

【識別番号】

100092196

【住所又は居所】

東京都千代田区霞が関 3 丁目 7 番 2 号 鈴榮特許
綜合法律事務所内

【氏名又は名称】

橋本 良郎

特願 2 0 0 3 - 4 0 0 7 2 4

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 3 0 7 8]

1. 変更年月日	2 0 0 1 年 7 月 2 日
[変更理由]	住所変更
住 所	東京都港区芝浦一丁目 1 番 1 号
氏 名	株式会社東芝